DOCTORAL (PhD) DISSERTATION

Dawei Song

Debrecen
2022

UNIVERSITY OF DEBRECEN

MARTON GÉZA DOCTORAL SCHOOL OF LEGAL STUDIES

ISSUES ON CYBERCRIME IN CHINA: THEORY AND PRACTICE

Candidate:

Dawei Song

Supervisor:

Dr. Sándor Madai
PhD

Doctoral Program: Changes in State and Law in Central and Eastern Europe

Head of the Doctoral School: Prof. Dr. József Szabadfalvi, DSc, Professor of Law

Manuscript completed on: 11 April 2022

DEBRECEN
2022

NYILATKOZAT

Alulírott, Song Dawei (név), büntetőjogi felelősségem tudatában kijelentem, hogy a Debreceni Egyetem Marton Géza Állam- és Jogtudományi Doktori Iskolában a doktori fokozat megszerzése céljából benyújtott, Issues on Cybercrime in China: Theory and Practice című értekezésem saját önálló munkám, a benne található, másoktól származó gondolatok és adatok eredeti lelőhelyét a hivatkozásokban (lábjegyzetekben), az irodalomjegyzékben, illetve a felhasznált források között hiánytalanul feltüntettem.

Kijelentem, hogy a benyújtott értekezéssel azonos tartalmú értekezést más egyetemen nem nyújtottam be tudományos fokozat megszerzése céljából.

Tudomásul veszem, hogy amennyiben részben vagy egészben sajátomként mutatom be más szellemi alkotását, vagy az értekezésben hamis, esetleg hamisított adatokat használok, és ezzel a doktori ügyben eljáró testületet vagy személyt megtévesztem vagy tévedésben tartom, a megítélt doktori fokozat visszavonható, a jogerős visszavonó határozatot az egyetem nyilvánosságra hozza.

Debrecen, 2022, April 11

aláírás

Supervisor's Recommendation

I recommend this doctoral dissertation under the title "Issues on Cybercrime in China: Theory and Practice," written by Song Dawei.

First of all, the topic of this doctoral dissertation is novel. Since the widespread popularization of computer information technology for civilian and commercial use in the 1990s, cybercrime has become one of the severe challenges that cannot be ignored in human society. On the one hand, the Internet has closely connected the entire earth unprecedentedly; on the other hand, the Internet has established a bridge between the virtual world and the real world. According to these two characteristics, on the one hand, cybercrime presents the characteristics of a global challenge, which requires all countries' joint efforts to participate and govern; on the other hand, it also offers a challenge to traditional criminal law. In other words, the existing legal system and governance methods are no longer compatible with the actual needs of responding to cybercrimes. Accordingly, this doctoral dissertation takes China's theory and practice of cybercrime governance as a starting point and provides China's experience and plans in the context of global cybercrime governance.

Second, this doctoral dissertation involves a wealth of criminological and sociological theories. This dissertation is based on the subject background of criminal law, combined with criminal law dogmatics, criminology and criminal policy, and discusses cybercrime from multiple angles. This dissertation starts with criminological perspectives and then provides a general criminological definition of cybercrime. At the same time sorts out the evolution and development of the popular academic term of cybercrime and shows us a clear context of the development of academic terms. At the same time, the author explained cybercrime based on Social Process Theory, Social Construction Theory and Social Conflict Theory and deepened the criminological cognition of cybercrime. In the specific practical discussion of China's response to cybercrime, the author also cited a series of criminological, sociological theories such as Crime Prevention Theory, Rational Choice Theory, Chivalry Theory, and Focal Concern Theory, demonstrating the author's rich and profound theoretical foundation.

Third, this doctoral dissertation sorts out China's legal system to deal with cybercrime in detail and provides us with relatively abundant and comprehensive background knowledge to understand the current state of China's policies and legislation controlling cybercrime in recent years. At the same time, the author discussed the dynamic interaction between China's

legislation controlling cybercrime in recent years. At the same time, the author discussed the dynamic interaction between China's Internet real-name system, combating online obscene live broadcasts and the responsibility of Internet sharing economic platforms and criminal governance of cybercrime through specific case studies.

Fourth, the structure of this doctoral dissertation is complete and reasonable. In writing this dissertation, the author progressively demonstrates the practice of China's governance of cybercrime through the process of criminal justice, which is specifically manifested in the practice of criminal legislation, the practice of conviction, and the practice of sentencing for cybercrime. This structural arrangement conforms to the fundamental rules of criminal law operation and the general logic of criminal governance.

Fifth, the research methods of this dissertation are relatively diverse. The author uses a relatively affluent research method in this doctoral thesis, including not only normative analysis methods, such as doctrinal analysis, case analysis, text analysis, etc.; but also empirical analysis methods, such as quantitative analysis, descriptive analysis, analysis of variance, and regression analysis, etc. These research methods show the author's interdisciplinary research ability and reflect the author's multi-angle and in-depth thinking and insights on the issue of cybercrime.

Information technology continues to advance, and cybercrime is also "advancing with the times." The research on cybercrime should be continuously deepened and enriched. This doctoral dissertation was produced during the author's four consecutive years of research on cybercrime and represents his hard work and dedication during his Ph.D. study. At the same time, this doctoral thesis also enriches the results of the research field of cybercrime.

This PhD dissertation meets the requirements.

Debrecen, 13 April, 2022

Dr. Sándor Madai

supervisor

ACKNOWLEDGEMENT

Time flies, doesn't it?

My doctoral studies at the University of Debrecen began four years ago. I'll never forget the four years I spent at this school.

At the University of Debrecen, I became acquainted with Marton Géza Doctoral School of Legal Studies professors. They are friendly, welcoming, and knowledgeable. My supervisor, Dr. Madai Sándor, helped me greatly in my studies and research. I was also fortunate enough to meet a wonderful group of fellow students during this unforgettable experience.

As of today, I have completed my doctoral dissertation. Graduation is just around the corner. I would like to express my appreciation to my supervisor, the faculty and staff of the Marton Géza Doctoral School, my fellow classmates, the University of Debrecen, and Hungary, a beautiful country with kind and passionate people.

Wishing for a bright future for my scientific research in China and a successful career there. I'll never forget my education at the University of Debrecen and the wonderful Hungarians who assisted and taught me there.

Song Dawei

at Damjanich utca 35, III-2

Debrecen, Hungary

April 11, 2022

TABLE OF CONTENTS

I. INTRODUCTION 1
1. THE ANTECEDENTS AND THE OBJECTIVES OF THE DOCTORAL DISSERTATION 1
2. RESEARCH STATUS OF CYBERCRIME IN CHINA 5
3. RESEARCH METHODOLOGIES APPLIED IN THIS DISSERTATION 10
4. RESEARCH LAYOUT AND STRUCTURE OF THIS DISSERTATION 11
5. NEW CONTRIBUTIONS TO ACADEMIC KNOWLEDGE 13
II. OVERVIEW OF CYBERCRIME 15
1. DEFINITION OF CYBERCRIME 15
1.1 VARIOUS TERMINOLOGIES 15
1.2 DEFINING CYBERCRIME 21
2. MORPHOLOGY OF CYBERCRIME 27
2.1 MORPHOLOGY OF CYBERCRIME IN GENERAL 28
2.2 MORPHOLOGY OF CYBERCRIME IN CHINA 34
3. CRIMINOLOGICAL THEORETICAL UNDERSTANDING OF CYBERCRIME: BASED ON THE SOCIOLOGICAL APPROACHES IN CRIMINOLOGY 39
3.1 SOCIAL STRUCTURE THEORY: STRAIN THEORY 42
3.2 SOCIAL PROCESS THEORY: DIFFERENTIAL ASSOCIATION THEORY AND SOCIAL LEARNING THEORY 50
3.3 SOCIAL CONFLICT THEORY: RADICAL CRIMINOLOGY AND FEMINIST CRIMINOLOGY 57
3.4 STAGED SUMMARY 67
III. LEGAL MEANS AGAINST CYBERCRIME IN CHINA: THE LEGISLATIVE PRACTICE 69
1. A GLANCE AT CHINESE LEGAL SYSTEM 69
1.1 SOCIALIST LEGAL SYSTEM WITH CHINESE CHARACTERISTICS 69
1.2 SOURCE OF LAW IN MAINLAND CHINA TODAY 71
1.3 A BRIEF DISCUSSION OF CHINA'S JUDICIAL INTERPRETATIONS 77
2. CYBER-POLICIES IN CHINA 78
2.1 THE MACRO LEVEL 79
2.2 THE MICRO ASPECTS 82
3. CYBERLAW IN CHINA 85
3.1 THE NARROW DEFINITION OF CYBERLAW IN CHINA 86
3.2 THE BROAD DEFINITION OF CYBERLAW IN CHINA 88
4. CYBERCRIMINAL LAW IN CHINA 92
4.1 CYBERCRIME IN THE CRIMINAL CODE AND ITS AMENDMENTS 93
4.2 CYBERCRIME IN THE JUDICIAL INTERPRETATIONS 95
4.3 JUDICIAL JURISDICTION OF CYBERCRIME IN CHINA 97
5. REGIONAL INTERNATIONAL COOPERATION AND CHINA'S CHOICE 102
5.1 SCO AND ITS MEMBER STATES 103
5.2 SCO'S COOPERATION IN CYBER AFFAIRS AND CHINA'S ROLE 104
5.3 COMMENTS AND DISCUSSIONS 108
IV. EVALUATIONS AND REFLECTIONS OF CHINA'S PRACTICE ON CYBERCRIME: THE CONVICTION PRACTICE 111
1. DYNAMIC BALANCE BETWEEN CYBERCRIME PREVENTION AND HUMAN RIGHTS

PROTECTION: REFLECTIONS ON THE INTERNET REAL-NAME SYSTEM IN CHINA *113*
1.1 INTERNET REAL-NAME SYSTEM: DEFINITION AND CATEGORY 114
1.2 RELATED MEASURES IN CHINA: LEGISLATIONS AND COMMENT 116
1.3 CRIME PREVENTION AND CYBERCRIME PREVENTION 120
1.4 DIALECTICAL RELATIONSHIP: INTERNET REAL-NAME SYSTEM AND CYBERCRIME PREVENTION 124
1.5 STAGED SUMMARY 136
2. THE PRINCIPLE OF LEGALITY IN CRIMINAL LAW AND EXPLANATION EXTENSION OF CURRENT LEGISLATION ON CYBERCRIME GOVERNANCE: REFLECTIONS ON COMBATTING ONLINE OBSCENE LIVE-STREAMING IN CHINA *137*
2.1 "CLEANNET 2019" CAMPAIGN AND REPRESENTATIVE CASES IN CHINA 139
2.2 COPING WITH ONLINE OBSCENE LIVE STREAMING IN CHINA 150
2.3 DISCUSSIONS: PROBLEMS IDENTIFIED AND STRATEGY CHOICES 155
2.4 STAGED SUMMARY 165
3. ECONOMIC INNOVATION PROTECTION AND CYBERCRIME GOVERNANCE: ONLINE PLATFORM OPERATOR'S CULPABLE POSSIBILITY IN THE INTERNET SHARING ECONOMY *166*
3.1 INTERNET SHARING ECONOMY AND ITS APPLICATION 166
3.2 DIDI CASES IN CHINA 167
3.3 CULPABLE POSSIBILITY AND ONLINE PLATFORM OPERATORS 170
3.4 STAGED SUMMARY 173
V. AN ANALYSIS OF SENTENCING DISPARITY AND AUXILIARY CYBERCRIME: THE SENTENCING PRACTICE 175
1. OVERVIEW *175*
2. LITERATURE REVIEW *181*
2.1 PRIOR RESEARCHES ON SENTENCING DISPARITY 181
2.2 THEORETICAL FRAMEWORKS ON EXPLAINING SENTENCING DISPARITY 184
3. METHODOLOGY *188*
3.1 DATA AND SAMPLING 188
3.2 VARIABLES 189
3.3 ANALYTICAL STRATEGY 193
4. FINDINGS *193*
4.1 DESCRIPTIVE ANALYSES 193
4.2 RESULTS OF MULTIVARIATE TESTS 195
4.3 RESULTS OF REGRESSION ANALYSIS 199
5. DISCUSSION AND STAGED SUMMARY *203*
5.1 DISCUSSION 203
5.2 STAGED SUMMARY 206
VI. CONCLUSIONS 209
APPENDIX I 218
APPENDIX II 220
APPENDIX III 224
BIBLIOGRAPHY 227
LIST OF PUBLICATIONS OF PH.D. CANDIDATE 266

I. INTRODUCTION

1. THE ANTECEDENTS AND THE OBJECTIVES OF THE DOCTORAL DISSERTATION

Nowadays, it's easy to think how inconvenient living in a time and space without the Internet would be. From the necessities of People's daily life to the social and economic development, and then to the high-tech competition between countries, all aspects of human society are accompanied by the shadow of the Internet. No one could have imagined at the time that the Advanced Research Projects Agency Network (ARPANET), funded by the U.S. Department of Defense to secure military communications during the Cold War, would evolve over decades into an Internet that would connect people around the world and have such a profound impact on the world as a whole.[1] From the popularity of the Internet for commercial and civil use in the mid-1990s to today[2], after more than 20 years of social changes and technological progress, people's demand for the Internet has developed from access to the Internet to open the door to a new world to more diversified experiences such as innovation and cybersecurity. Technological development is also actively responding to people's needs at more levels, mainly reflected in the popularity of a series of information network technology concepts in recent years, such as Meta-universe[3], 5G, Artificial Intelligence, Big Data, Blockchain, Cloud Computing and so on. However, the progress of information network technology cannot solve the fundamental malpractice of the Internet --- cybercrime.

Cybercrime has been around since the dawn of the Internet. Before the formal commercial and civilian adoption of the Internet, especially in the United States, it mainly existed in local area networks (LANs) and was used primarily between national security systems, high-tech information systems, and universities.[4] The birth and initial development

---

[1] BARRY M. LEINER, VINTON G. CERF, DAVID D. CLARK, ROBERT E. KAHN, LEONARD KLEINROCK, DANIEL C. LYNCH, JON POSTEL, LARRY G. ROBERTS AND STEPHEN WOLFF: *Brief History of the Internet*. Internet Society, 11 November 2021. https://www.internetsociety.org/internet/history-internet/brief-history-internet/

[2] MAJID YAR: *Cybercrime and Society*. Sage, 2013. 2nd Edition, p. 20.

[3] DAN MILMO: *Enter the Metaverse: The Digital Future Mark Zuckerberg is Steering us Toward*. The Guardian, 11 November 2021. https://www.theguardian.com/technology/2021/oct/28/facebook-mark-zuckerberg-meta-metaverse

[4] SUSAN W. BRENNER: *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston, Northeast University Press, 2012. Chapter 1.

of computers make a group of college students interested in it. However, due to the scarcity and high cost of computers and the closed nature of information networks at the initial stage, these college students with strong interest and enthusiasm in computers and networks cannot get corresponding opportunities to get close to and understand computers and networks. Therefore, sneaking into these closed computer systems seemed the only chance for students who have no direct access to computers to learn about computer networks. It is also the embryonic form of hacking of cybercrime.[5] With the iterative innovation of technology and the popularization and development of the Internet, cybercrime itself is constantly "evolving." As a result of this evolution, cybercrime, which was initially a by-product of information networks, can now directly affect the development of information networks. In other words, people's anxiety about cybercrime has directly affected their acceptance and tolerance of the Internet.

Every year, governmental agencies of many countries, international organizations, cybersecurity enterprises, academic groups have made reports on the specific indicators of harm caused by cybercrime, such as economic losses, distribution of cybercrime victims, and the number of cybercrimes. For example, from a global perspective, the *2020 Internet Crime Report* published by the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation in the United States noted that: Over the last five years (2016-2020), the IC3 had received 2,211,396 complaints across the globe in total. These cybercrime complaints amounted to a total economic loss of 13.3 billion dollars.[6] In terms of Cybercrime in China, at the 4th Session of the 13th National People's Congress in 2021, the Work Report of the Supreme People's Court showed that China's courts had trialed 33,000 cybercrime cases in 2020.[7] According to the Work Report of the Supreme People's Procuratorate, China's procuratorial system prosecuted 142,000 people for cybercrime in 2020, up 47.9 percent year-on-year amid a decline in the total number of criminal cases.[8]

Taken as a whole, the release of these reports indicates a high level of social concern

[5] STEVEN LEVY: *Hackers: Heroes of the Computer Revolution*. New York, Anchor Press/Doubleday, 1984. pp. 18-69.

[6] INTERNET CRIME COMPLAINT CENTER (IC3): *2020 Internet Crime Report*. Federal Bureau of Investigation, 11 November 2021. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[7] QIANG ZHOU: *Work Report of the Supreme People's Court of 2021*. The Supreme People's Court of The People's Republic of China, 21 November 2021, http://www.court.gov.cn/zixun-xiangqing-290831.html

[8] JUN ZHANG: *Work Report of the Supreme People's Procuratorate of 2021*. The Supreme People's Procuratorate of The People's Republic of China, 21 November 2021, https://www.spp.gov.cn/spp/gzbg/202103/t20210315_512731.shtml

about cybercrime. On the one hand, such increasing attention shows that the rising harm degree of cybercrime has to attract society's attention. On the other hand, it also indicates the consensus reached by governments worldwide, different international organizations, and social organizations: cybercrime urgently demands governance.

Generally speaking, cybercrime governance means that the country uses a series of legal means, such as legal policies, legislation, law enforcement, judicial, and non-legal means, such as social policies, to reduce and deal with the occurrence of cybercrime, remedy the infringement caused by cybercrime, and finally achieve the effect of cybercrime control. In recent years, cybercrime governance has become an essential part of the world's crime governance. On the one hand, countries worldwide strengthen cybercrime control by constantly improving policies, management, and cyber legislation, such as the *Cybersecurity Enhancement Act of 2014*, *Cybersecurity Information Sharing Act of 2015*, *Federal Exchange Data Breach Notification Act of 2015*, and *National Cybersecurity Protection Advancement Act of 2015* in the United States. On the other hand, in response to cybercrime globalization, international and regional organizations and treaties are also constantly improving the legal network of cybercrime control. For example, on 14 April 2016, European Union adopted the *General Data Protection Regulation*.

Of course, the global governance of cybercrime based on the guiding ideology of building a community of human cyberspace is inseparable from China's practice and lessons. Since the *Reform and Opening-up Policy* was adopted in the late 1970s, China has made significant economic and social development progress. As the largest developing country in the world, according to the statistics of the World Bank in 2020, China's WORLD GDP Ranks only next to the United States and the European Union, making China the third-largest economy in the world.[9] In recent years, the Chinese government has advocated the transformation of economic development mode and begun to attach importance to the positive role of the Internet in economic and social construction. The concept of "Internet Plus" was first proposed by Chinese Premier Li Keqiang in the *Government Work Report of 2015*. Specifically, the "Internet plus" action plan is formulated to promote the combination of mobile Internet, cloud computing, big data, and Internet of Things (IoT) with modern manufacturing, promote the healthy development of e-commerce, industries, and finance, and

[9] THE WORLD BANK: *GDP Ranking: Gross Domestic Product Ranking Table*. The World Bank, 12 November 2021. https://datacatalog.worldbank.org/search/dataset/0038130/GDP-ranking

guide Internet enterprises to expand the international market.[10] In the *Government Work Report of 2020*, Premier Li Keqiang reiterated and stressed the importance of "Internet Plus" in an all-around way to create new advantages of the digital economy.[11] Under the government's advocacy of the Internet, China's social economy is increasingly showing the characteristics of Internet integration. It has created representative "business cards" with Chinese features, such as sharing economy, mobile payment, 5G technology, Tik Tok. The high affinity of the Chinese economy and society to the Internet, on the one hand, promotes the vigorous development of Internet technology in China; on the other hand, it also brings risks and challenges -- an increasingly high incidence of cybercrime.

To cope with the risks and challenges brought by cybercrime and protect the development of China's Internet economy, China is constantly taking a litany of measures to achieve cybercrime governance. In particular, over the past decade, Chinese leaders have repeatedly issued statements in the international community on combating cybercrime and safeguarding cybersecurity. At the same time, China is constantly revising existing laws and formulating new laws, regulations, and policies to improve the governance capacity of cybercrimes. China's cybercrime governance practice has achieved remarkable results. According to the Law-and-Order Index of Gallup, China ranks the third safest country globally.[12] The ranking can be interpreted as saying that China is one of the safest countries in the world (including cybersecurity recognition).[13] It is worth mentioning that China is the most populous country in the world. Chinese people's high evaluation of China's security experience based on law and order also reflects the achievements of China's cybercrime governance practice from one side. Therefore, it is of positive learning significance to discuss China's cybercrime governance practice and experience in the context of global cybercrime governance. Furthermore, nothing in the world is perfect, nor is China's practice of cybercrime control. It is also of reference significance to fully understand cybercrime governance through discussions of the shortcomings in the praxis of China's cybercrime governance.

---

[10] LI KEQIANG: *Government Work Report of 2015*. The State Council of People's Republic of China, 11 November 2021. http://www.gov.cn/guowuyuan/2015-03/16/content_2835101.htm

[11] LI KEQIANG: *Government Work Report of 2020*. The State Council of People's Republic of China, 11 November 2021. http://www.gov.cn/guowuyuan/2020zfgzbg.htm

[12] JULIE RAY: *Most of the World Remains Confident in Police, Feels Safe*. Gallup Inc., 12 November 2021. https://news.gallup.com/poll/322565/world-remains-confident-police.aspx

[13] CCTV NEWS: *China is "one of the most secure countries in the world" The national public security index in 2020 is 98.4%*. CCTV. COM, 12 November 2021. https://news.cctv.com/2021/04/15/ARTIAuqN0sAjdiQh6rGWd15y210415.shtml

To sum up, this dissertation takes the issues of cybercrime in China as the theme. By sorting out, analyzing, and discussing the practice of cybercrime governance in China and summarizing the issues in China's practice, the following research objectives can be achieved:

(a) Develop a criminological definition of cybercrime and a holistic understanding of cybercrime.

(b) Summarize and assess China's domestic and regional international legal mechanisms for governing cyberspace and cybercrime.

(c) Analyze and summarize China's conviction practice and experience with cybercrime governance.

(d) Conduct research and analysis on the practice and current state of sentencing in China's cybercrime governance.

2. RESEARCH STATUS OF CYBERCRIME IN CHINA

As the topic of this dissertation is about the issues of cybercrime governance in China, this part focuses on sorting out the research status of Chinese scholars on cybercrime. What needs to be distinguished is that this part believes that research status is not equal to literature review. A literature review integrates and reflects research results in a specific research field based on extensive reading and understanding of the literature. Literature review needs to summarize and comment on the retrieved literature and put forward the researcher's own opinions.[14] The writing requirements of research status are not as cumbersome as the literature review. The research status is mainly to sort out and analyze the main viewpoints (topics) of the existing research results, the previous research level, the focus of debate, the current problems, and so on. The basic structure of this part is "bibliometric analysis + characteristic summary." This part focuses on the macroscopic grasp of Chinese academic research on cybercrime.

The literature source of this part is the CNKI database of China. This part is searched in the CNKI database with the topic of "cybercrime." As cybercrime itself is developing, academic research on it is also constantly updated. Therefore, this part limited the time interval of literature publication and finally took the research results of the last decade as the main object of sorting, namely 2011-2020. This part mainly selects two levels of research-

[14] JUSTUS RANDOLPH: A Guide to Writing the Dissertation Literature Review. *Practical Assessment, Research, and Evaluation*, vol. 14. no. 13. (2009) 1-14.

level: articles on cybercrime in Chinese core journals of Chinese Social Science Citation Index (CSSCI) and doctoral dissertations on cybercrime.

Five hundred and thirty (530) valid samples were obtained by searching the database and screening the retrieval results, with 27 doctoral dissertations accounting for 5.1% of the total sample; 503 articles on CSSCI core journals accounted for 94.9% of the total sample. Through the bibliometric analysis and classification analysis of these 530 samples, this part found that:

Overall Publication of Chinese Scholars in Sample by YEAR					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2011	16	3.0	3.0	3.0
	2012	27	5.1	5.1	8.1
	2013	30	5.7	5.7	13.8
	2014	36	6.8	6.8	20.6
	2015	38	7.2	7.2	27.7
	2016	61	11.5	11.5	39.2
	2017	84	15.8	15.8	55.1
	2018	60	11.3	11.3	66.4
	2019	96	18.1	18.1	84.5
	2020	82	15.5	15.5	100.0
	Total	530	100.0	100.0	

Table I. 2-1 Overall Publication of Chinese Scholars in Sample by YEAR

(1) Chinese scholars' attention to cybercrime research has generally shown an increasing trend year by year. From 2011 to 2020, the number of publications of Chinese scholars on cybercrime, cyber law, or cyberspace governance has increased year by year. For details, please refer to Table I. 2-1.

(2) In terms of research methodology, Chinese scholars tend to adopt the normative analysis method compared with the positive analysis method. Specifically, there were 489 studies, accounting for 92.3%, based on the normative analysis approaches. There were 41 studies mainly based on the positive analysis approaches, accounting for 7.7%.

(3) In terms of research themes, there are 226 studies involving cyber policies, accounting for 42.6% of the total; 93 studies involving cyber law, accounting for 17.5%; 407 studies involving cybercriminal law science, accounting for 76.8%. In addition, there were 61 studies involving both cyber policy and cyber law, 104 studies involving both cyber policy and cybercriminal law science, seven (7) studies involving cyberlaw and cybercriminal law science, and 16 studies covered all three topics.

(4) In terms of research form, there were 186 items, including criminal law dogmatics, accounting for 35.1% of the total sample; 76 items, including the exploitation to crime,

accounting for 14.3%; 50 items, including the explanation of crime, accounting for 9.4%; 202 items, including the response to crime, accounting for 38.1%; 42 items, including the form of criminal justice, accounting for 7.9%.

(5) In terms of research content, there are 129 macroscopically related studies on policies and practices of cyberspace governance in the sample, accounting for 24.3%. There were 250 studies related to cybercriminal policy and governance, accounting for 47.2%; 103 items related to the basic criminal law theory, accounting for 19.4%.

(6) In terms of research objects, 135 studies involving existing offenses in China's Criminal Code, accounting for 25.5%. There were 32 studies on the criminalization of cyber deviance not stipulated by criminal law, accounting for 6.0%.

(7) In terms of studying the impact of the Internet on the traditional normative system, 117 studies concerned the cyber-alienation on traditional crimes, accounting for 22.1%. Forty-four (44) studies involved the online challenges to traditional rights, accounting for 8.3%.

(8) In terms of the subject characteristics in the research, there were 500 studies on the general criminal subjects, accounting for 94.3%; There were 30 studies on minorities, such as minors, university students, and ethnic minorities, accounting for 5.7%.

(9) Regarding the internationalization of research, there were 75 studies covering governance practices in international and non-Chinese regions, accounting for 14.2%; 455 studies focused only on governance practices in mainland China, accounting for 85.8%. Among them, 76 studies involved introducing, reviewing, and promoting China's cyberspace governance policies, accounting for 14.3%; 128 studies involved introducing, reviewing, and promoting China's criminal policies of cybercrime, accounting for 24.2%; 261studies involved introducing, reviewing, and advancing China's legislation on cyberlaw or cybercriminal law, accounting for 49.2%.

Based on collecting, analyzing, and researching the results of the bibliometric analysis and classification analysis of sampled literature, this part holds that Chinese scholars' research on cybercrime in the past decade (2011-2020) presents the following characteristics:

First, more emphasis is placed on the response to cybercrime, and less attention is paid to the explanation of cybercrime (the use of criminological theory to explain cybercrime

research[15]). Chinese scholars' research on the response to cybercrime was relatively concentrated in the study of cybercriminal law science. There was a significant correlation between the study of cybercriminal law science and the response to cybercrime (χ^2=51.519, p=.001, α=.05). Meanwhile, there was a significant correlation between the response to cybercrime and the form of criminal justice (χ^2=13.247, p=.001, α=.05). It indicates that the research on criminal justice of cybercrime is usually inclined to discuss the response to cybercrime. In other words, Chinese scholars generally study the criminal justice issues of cybercrime to realize the governance of cybercrime.[16]

[15] (Although Chinese scholars rarely use criminological theories to explain cybercrime, this part still selects some representative studies from the samples.) e.g., See. ZEGANG JIN AND YA'AN WU: The Influence of Online Games on Juvenile Delinquency: An Explanation Based on Social Control Theory [网络游戏对青少年犯罪的影响：一种基于社会控制理论的解释]. *Issues on Juvenile Crimes and Delinquency* [青少年犯罪问题], no. 5. (2012) 75-82; HUIBO WANG: Social Learning Theory of Our Country from the Perspective of White-Collar Crime Analysis [社会学习理论视角的我国白领犯罪解析]. *Henan Social Science* [河南社会科学], vol. 20. no. 8. (2012) 52-55; SHUGUANG YUAN: Sociological Analysis of Crime of Internet Pornography, Gambling and Drugs [网络黄赌毒犯罪的社会学分析]. *Dongyue Tribune* [东岳论丛], vol. 33. no. 7. (2012) 179-181; YONG ZENG, XIAOJIANG LI AND WENQI ZHAO: Detection Model of Concealed Conspiracy in Enterprise Based on Social Network Analysis and Fuzzy Comprehensive Evaluation Method [基于社会网络分析的企业隐藏犯罪探测的模糊评价模型]. *Journal of Modern Information* [现代情报], vol. 32. no. 7. (2012) 103-106; HONG LI: Situational Criminology and Criminal Law Concept of Prevention [情境犯罪学与预防刑法观]. *Law Review* [法学评论], vol. 36. no. 6. (2018) 15-28; YONGSHENG LI AND WEI WU: Crime Theory of Campus Bully and Its Prevention and Control Strategies: Taking China's 100 Online News in Recent Three Years as Research Samples [校园欺凌的犯罪学理论分析与防控策略：以我国近 3 年 100 件网络新闻报道为研究样本]. *Journal of Shandong University (Philosophy and Social Sciences)* [山东大学学报(哲学社会科学版)], no. 1. (2019) 65-74; XU ZHANG AND XIAOYAN ZHU: Crime Governance in Weak Smart Society: Situation, Dilemma, and Settlement Paths [弱智慧社会语境下的犯罪治理：情势、困境与出路]. *Jilin University Journal Social Sciences Edition* [吉林大学社会科学学报], vol. 59. no. 1. (2019) 19-29+219; YANA LIU AND YINGTONG GAO: An Empirical Study of Juvenile Delinquency Due to Addiction to Online Games and Its Coping Mechanism [青少年沉迷网络游戏及引发犯罪的实证研究与应对机制]. *Journal of Shandong University (Philosophy and Social Sciences)* [山东大学学报(哲学社会科学版)], no. 3. (2020) 9-21.

[16] e.g., See. YONGSHENG CHEN: The Challenge and System Response of Cybercrime to Criminal Procedure [计算机网络犯罪对刑事诉讼的挑战与制度应对]. *Science of Law (Journal of Northwest University of Political Science and Law)* [法律科学(西北政法大学学报)], vol. 32. no. 3. (2014) 140-153; XIAOMING LI AND WENJI LI: Criminal Jurisdiction Analysis of Transnational Cybercrime [跨国网络犯罪刑事管辖权解析]. *Journal of Soochow University (Philosophy & Social Science Edition)* [苏州大学学报(哲学社会科学版)], vol. 39. no. 1. (2018) 89-100; WEI PEI: The Connection of the Electronic Forensics Rules before and after Criminal Recording: From the Perspective of Procedural Nature of Electronic Evidence [刑事立案前后电子取证规则衔接问题研究：以电子数据证据过程性为视角]. *Contemporary Law Review* [当代法学], vol. 33. no. 2. (2019) 114-126; LIMEI WANG: The Construction of Summary Procedure of Judicial Assistance of Cross Border Electronic Evidence [论跨境电子证据司法协助简易程序的构建]. *Law Science Magazine* [法学杂志], vol. 41. no. 3. (2020) 82-92; DENGKE XIE: Rethink and Reconstruction of the Online Extraction Rules of Electronic Evidence [电子数据网络在线提取规则反思与重构]. *Oriental Law* [东方法学], no. 3. (2020) 89-100; DAN SHAN AND LAI WANG: The Application of Big Data in the

Second, from a comprehensive perspective of the basic criminal law theory and the involvement of crimes in China's Criminal Code, the research form of criminal law dogmatics occupies a relatively dominant position. There was a significant correlation between the research form of criminal law dogmatics and offenses in China's Criminal Code (χ^2=130.188, p=.001, α=.05). It can be interpreted as that the research object of Chinese scholars' criminal law dogmatics of cybercrime is usually the offenses stipulated in the current Chinese Criminal Legislation or usually involves the provisions of the specific Criminal Code. At the same time, there was a significant correlation between the research form of criminal law dogmatics and the basic criminal law theory (χ^2=189.522, p=.001, α=.05). It could be understood that Chinese scholars focused not only on specific offenses in Criminal Code but also on the study and interpretation of cybercrimes from the perspective of basic criminal law theories, such as the theory of accomplice.[17]

Third, it focused on international governance of cybercrime and non-Chinese practices and lessons. Chinese scholars' research on the internationalization of cybercrime was significantly correlated with cyberspace governance practice (λ=.364, p=.001, α=.05), but not with cybercrime governance and the cybercriminal policy (λ=.052, p=.542, α=.05). It indicated that the internationalization studies of Chinese scholars usually focus on cyberspace governance practice internationally or abroad[18] and less on the governance and criminal

---

Investigation of Online Illegal Fund-Raising Cases [大数据在网络非法集资案件侦查中的应用]. *Journal of People's Public Security University of China (Social Sciences Edition)* [中国人民公安大学学报(社会科学版)], vol. 33. no. 4. (2017) 84-91.

[17] e.g., See. TIENAN MI: The Dilemma of Accomplice Theory in Computer Network Crimes and Its Solutions [共犯理论在计算机网络犯罪中的困境及其解决方案]. *Jinan Journal (Philosophy & Social Sciences)* [暨南学报(哲学社会科学版)], vol. 35. no. 10. (2013) 3-63+161; LIN WANG: Shaping from Dogmatics for Criminal Liability Mode for Participative Conduct of Cybercrime [网络犯罪参与行为刑事责任模式的教义学塑造：共犯归责模式的回归]. *Political Science and Law* [政治与法律], no. 9. (2016) 30-42; YUNLIANG SUN: Dogmatics Introspection on the Principal Offenderization of Helping Behavior [帮助行为正犯化的教义学反思]. *Journal of Comparative Law* [比较法研究], no. 6. (2018) 120-133; YICHENG DENG: Can Theory of Accessorial Accomplice Be Applied in Transformed Principal? [共犯正犯化背景下的从属性困境及理论应对]. *Peking University Law Journal* [中外法学], vol. 31. no. 3. (2019) 780-796; SANYANG LIU AND CE QIN: On the Model of Cybercrime Accomplice Regulation Independent Governance [网络犯罪共犯规制独立化治理模式论]. *Chongqing Social Sciences* [重庆社会科学], no. 7. (2019) 89-98+82; SUZHI WANG: On the Principal Quality of Cybercrime Participation: Rethinking Based on the Offence of Assisting Cybercrime [论网络犯罪参与行为的正犯性：基于帮助信息网络犯罪活动罪的反思]. *Journal of Comparative Law* [比较法研究], no. 1. (2020) 170-184.

[18] e.g., See. YINGYING XIAO AND ZHENGQING YUAN: A Primary Exploration on Cyber Security Governance in Africa [非洲网络安全治理初探]. *West Asia and Africa* [西亚非洲], no. 3. (2016) 121-137; WEI SUN AND QICHAO ZHU: A Primary Study on ASEAN Cyber Security Cooperation [东盟网络安全合作现状与展望]. *Southeast Asian Studies* [东南亚研究], no. 1. (2016) 56-64; WEI WANG: Singapore's

policies of cybercrime.

Fourth, Chinese scholars have recognized the impact of the uniqueness of cyberspace on the real world. It is manifested as both the influence on traditional crime and rights and the salience of minority groups. And studying this effect requires a different approach. There is a significant correlation between the study of juvenile or minority groups and the response to crime (χ^2=4.641, p=.031, α=.05). It indicates that Chinese scholars' research on cybercrime for minors and minority groups usually focuses on the response to cybercrime of such notable groups, manifested explicitly in particular groups' crime prevention and regulation.[19]

Finally, it is relatively insufficient that only 16 studies concerned cyber policy, cyber law, and cybercriminal law together, accounting for 3.01% of the total sample. It is also an essential embodiment of the research significance of this doctoral thesis.

3. RESEARCH METHODOLOGIES APPLIED IN THIS DISSERTATION

In general, the research methods of this dissertation include normative analysis and empirical analysis. Specifically:

Chapter II mainly adopts literature analysis, comparative analysis, and legal doctrines in the overview of cybercrime. By sorting out the different definitions of cybercrime in various studies and combining them with comparative discussions, this chapter redefines cybercrime from the perspective of criminology. This chapter sorts out different theories on the morphological classification of cybercrime and discusses the morphology of cybercrime in China in combination with the specific provisions and legal doctrines of China's criminal

---

Cyberspace Governance and Its Enlightenment to China [论新加坡网络空间治理及对中国的启示]. *Pacific Journal* [太平洋学报], vol. 26. no. 2. (2018) 35-45; SHANPIN XU AND SHUCHENG WANG: Australia's Cyber Security Strategy in the Digital Age: New Connotation and New Trend [澳大利亚网络安全战略的新内涵与新动向]. *Journal of International Security Studies* [国际安全研究], vol. 37. no. 6. (2019) 104-128+155-166; CHUNRONG ZHENG AND XIAOSHAN NI: EU Cybersecurity Strategy and China-EU Cooperation [欧盟网络安全战略及中欧合作]. *Journal of Tongji University (Social Science Section)* [同济大学学报(社会科学版)], vol. 31. no. 4. (2020) 42-56.

[19] e.g., See. ZHONGHE LI: On Cyber Crimes of College Students and Its Prevention and Control Strategies [高校学生网络犯罪及其防控对策探讨]. *Science Economy Society* [科学·经济·社会], vol. 30. no. 2. (2012) 74-78; ZHIPING YANG: An Analysis of Adolescent Cyber Pornography Consciousness [青少年网络色情犯罪意识生成分析]. *Youth Exploration* [青年探索], no. 4. (2014) 84-88; HONGMEI DENG: Current Situation, Recognition and Prevention About Network Pyramid Selling Crime in Nationality Areas [民族地区网络传销犯罪的现状、识别及预防]. *Guizhou Ethnic Studies* [贵州民族研究], vol. 38. no. 4. (2017) 36-39; ZHENHUI WANG: The Crime of Minor's Social Networking: Risk Type and Prevention Measures [未成年人网络社交中的犯罪被害：风险类型与防范之策]. *Journal of Chinese Youth Social Science* [中国青年社会科学], vol. 39. no. 6. (2020) 120-127; YANA LIU and YINGTONG GAO, 2020, pp. 9-21.

law. Finally, Chapter II compares and evaluates the advantages and disadvantages of different criminological frameworks in understanding and explaining cybercrime by sorting out various criminology theories and their applications in cybercrime.

Chapter III mainly adopts literature analysis, historical analysis, descriptive analysis, and institutional analysis in China's legal means of cyberspace and cybercrime governance. Chapter III introduces the basic characteristics of China's legal system through institutional analysis. Second, through legal search and literature analysis, this chapter collects relevant policy documents and legal texts in China and analyzes and describes the content and characteristics of laws related to cyberspace governance and cybercrime governance. Meanwhile, Chapter III examines the evolution of legislation to protect the same legitimate rights and interests in China's legal system and introduces and comments on the evolution of China's legal system of cybercrime governance in chronological order. Finally, Chapter III mainly presents the current situation of China's participation in regional international cooperation in the governance of cyber affairs through the literature analysis and descriptive analysis of the SCO treaties and declarations. Chapter III does not look at the representations of various laws and policies in isolation but systematically analyzes China's cybercrime governance policies, rules, and regulations to reflect the coherence of policies and legislation.

Chapter IV mainly adopts literature analysis, legal dogmatics, qualitative analysis, functional analysis, and case analysis in the reflection and evaluation of the conviction practice of China's cybercrime governance. In researching cybercrime policy and human rights protection, this section focuses on legal dogmatics and functional analysis and discusses the balance between the Internet real-name system and cybercrime prevention and human rights protection. In researching the extension of the criminal law interpretation of cybercrime, this section emphasizes case analysis and qualitative analysis. It explores the conflict and way out between China's crackdown on online obscene live streaming crimes and the principle of legality in criminal law. In researching the direction of cybercrime legislation and policy, this section mainly uses case analysis, legal dogmatics, and qualitative analysis to explore the culpable possibility of online platform operators and the legislative direction and policy options to protect the Internet sharing economy.

Chapter V mainly adopts theoretical analysis, case analysis, descriptive statistical analysis, correlation analysis, and regression analysis in the research on the sentencing practice of China's cybercrime governance. Chapter V takes the Chinese cybercrime sentencing disparities in judicial practice as the main research object. Chapter V establishes

the theoretical framework to guide the research through theoretical analysis and literature analysis first; through case analysis, which establishes the research sample; through descriptive, correlation, and regression analysis, which studies both the legal and extra-legal factors affecting sentencing disparities of cybercrime in China's judicial practice.

4. Research Layout and Structure of This Dissertation

This dissertation consists of six chapters. Details are as follows:

The first chapter is the introduction. The first chapter mainly introduces the research background, research significance, research method, research layout and writing structure, as well as the new contribution of this research.

The second chapter provides an overview of cybercrime. The second chapter is mainly composed of three parts: the first is to redefine cybercrime from a criminological perspective. The second is to study the morphology of cybercrime. The third is the understanding and interpretation of cybercrime by sociological approaches in criminology.

The third chapter researches the legal means system of China's governance of cyberspace and cybercrime. The third chapter studies China's current legal means for cyberspace and cybercrime governance from domestic and regional international dimensions. Specifically, the third chapter mainly includes five parts: First is the basic characteristics of China's legal system. The second is China's cyber policies on the governance of cyberspace and cybercrime. The third is China's cyber law. Fourth is China's cybercriminal law. The fifth is the status quo of China's participation in regional international cyber affairs governance based on the Shanghai Cooperation Organization.

The fourth chapter researches the conviction practice of China's cybercrime governance. The fourth chapter is mainly based on China's current cybercriminal policy and criminal legislation doctrine. The fourth chapter mainly includes three parts: The first is to study the dynamic balance between cybercrime prevention and human rights protection. This part mainly reflects and evaluates China's Internet real-name system. By analyzing the legislative evolution of the Internet real-name system and its specific application in China, this part discusses its role in preventing cybercrime and its impact on human rights protection. The second is to study the principle of legality in criminal law and the explanation's extension of the current criminal legislation. This part mainly reflects and evaluates China's crackdown on online obscene live streaming crimes. Through the analysis of specific cases and the theoretical analysis of relevant legislation, this part discusses the direction of

explanation and extension of current criminal legislation and its relationship with the principle of legality in criminal law. The third is to study the cybercrime governance and culpable possibility of online platform operators under the Internet sharing economy. This part mainly analyzes the case of DiDi in China. By analyzing the culpable possibility of online sharing economy platform operators, this paper explores the relationship between the future direction of cybercrime governance and ensuring the healthy development of the Internet (economy and technology) in accordance with Chinese criminal law.

The fifth chapter researches the sentencing practice of China's cybercrime governance. Chapter V focuses on empirical evidence regarding the criminal justice practice of the *Crime of illegal utilization of information network technology* [Article 287(I)] and the *Crime of provision of assistance to conduct the cyber-criminal activity* [Article 287(II)] as stipulated in Amendment (IX) of Chinese criminal law. Chapter V summarizes the above two offenses as auxiliary cybercrime. The empirical analysis of criminal justice practice involved in the fifth chapter mainly studies the sentencing disparities of auxiliary cybercrime in China's criminal justice practice. The fifth chapter draws the following conclusions through the statistical analysis of more than 200 cybercrime assisted judgments from 2015 to 2019: the three main factors affecting the disparity in sentencing of cybercrime in China's criminal justice practice include the gender of the offender (an extra-legal factor), the court location (an extra-legal factor) and the seriousness of the cybercrime (a legal factor).

The sixth chapter summarizes the research findings from each chapter, then synthesizes and sublimates them in light of the entire doctoral dissertation's research content, and finally concludes with some experiences and lessons learned about China's cybercrime governance.

5. New Contributions to Academic Knowledge

This doctoral dissertation focuses on issues of cybercrime in China. The following are the novel contributions of this study to the field of cybercrime and China research:

The first is the breadth of research methods. This dissertation employs both normative and empirical analysis techniques. It emphasizes qualitative legal research techniques such as literature and comparative analysis and quantitative legal research techniques such as statistical analysis.

Second, the content of the research is relatively recent. This dissertation primarily examines the experience and lessons learned in China's recent ten-year history of cybercrime

governance.

Thirdly, the research structure is fairly well-developed. The research for this dissertation on China's cybercrime governance encompasses policies, laws and regulations, judicial practice, and the entire process of cybercrime criminal governance.

Fourth, the research is interdisciplinary, encompassing criminal law doctrine and other fields of criminal law science, such as criminal policy and criminology.

Fifth, the dissertation's central concept is global cybercrime governance. This dissertation examines and summarizes China's practice in light of global governance to develop a Chinese solution for global cybercrime governance.

II. OVERVIEW OF CYBERCRIME

Definitions, Morphologies & Theoretical Understandings on Cybercrime

This chapter's content is divided into three sections. The first aspect is how cybercrime is defined. The definition section introduces, categorizes, and summarizes three distinct cybercrime terminologies; then, through the development and evolution of these terminologies, the perception of cybercrime by government agencies and academics is revealed. The second aspect is about cybercrime's morphologies, particularly in China. The morphological section will introduce various classifications of cybercrime. The discussion will then shift to China's context. The morphologies of cybercrime in China will be introduced and briefly analyzed in light of the provisions and offenses in China's Criminal Law. The third aspect provides a theoretical framework for understanding cybercrime through the lens of Sociological Criminology. This part stands on the perspective of comprehensive governance of cybercrime, utilizing Strain Theory, Social Learning Theory/Differential Association Theory, Feminist Criminology, and Radical Criminology to explain and comprehend the impact of personal and social factors on cybercrime. Additionally, some comments and applications are discussed.

1. DEFINITION OF CYBERCRIME

1.1 VARIOUS TERMINOLOGIES

Cybercrime appears to be the most alien term. Cybercrime can also be perceived by someone who does not study it or has no background in law or criminology. Cybercrime is frequently associated with the following keywords: hackers, high-tech, computers, and so on. However, when cybercrime is used as the research object, this imprecise generalization becomes less rigorous. Typically, the definition of cybercrime reflects the times, the evolution of technology, and the evolution of cybercrime itself. There are three widely accepted definitions of cybercrime in the numerous studies on the subject: computer crime, high-tech crime, and cybercrime.

1.1.1 Computer Crime

The popularization of computers brings the abuse of computers into focus. Accordingly, authorities and scholars began to criminalize computer abuse. At first, people attempted to define computer crime by defining computers. However, this approach ultimately failed. For example, the *Computer Abuse Act of 1990* in the United Kingdom was

unable to define computers. The Law Commission believed that all tentative definitions were so complicated that they would cause widespread controversy, which would affect their application in judicial practice.[20]

Subsequently, scholars avoided giving a precise definition of computer crime directly but instead defined it in terms of general patterns of computer abuse: [i]n general, computer crimes consist of volitional, nonviolent acts involving a computer.[21] This avoidance of direct, precise definitions has gained traction. A more mature portrayal of computer crime has since emerged. For instance, computer crime has been used to refer to criminal activities involving a computer that is made illegal through the statute. A computer crime would be a crime that (a) the computer as an instrument of the crime; (b) the computer as the focus of a crime; (c) the computer as a repository of evidence.[22]

The first national official definition of *computer crime* might be in Senate Bill S.240, the *Federal Computer System Protection Act of 1979*, in the United States. In this bill, the *computer crime* should be any computer utilization for a fraudulent purpose, intentional, unauthorized use, access, or alterations of computer programs or data, and contains definitions of various terms used in the bill. Some scholars fiercely opposed this bill and seemed it had no meaning to be promulgated because the existing law can address all the problems referred to in the articles.[23]

However, in 1984, the United States passed the *Computer Fraud and Abuse Act (CFAA)*[24], and its content was similar to Senate Bill S.240. Subsequent studies have shown that computer crime does not seem to be entirely solved by existing laws. Computer crime generally includes any traditional offenses committed using a computer and encompasses new crimes against intellectual property and a category of previously unknown crimes that do not fit well into conventional criminal statutes.[25]

---

[20] RIZGAR MOHAMMED KADIR: The Scope and the Nature of Computer Crimes Statutes: A Critical Comparative Study. *German Law Journal*, vol. 11. no. 6. (2010) 609-632.

[21] ROBERT M. COUCH: A Suggested Legislative Approach to the Problem of Computer Crime. *Washington & Lee Law Review*, vol. 38. no. 4. (1981) 1173-1194.

[22] ROBERT MOORE: *Cybercrime: Investigating High-technology Computer Crime*. New York, Routledge, 2015. 2nd edition.

[23] JOHN K. TABER: On Computer Crime (Senate Bill S. 240). *Computer/Law Journal*, vol. 1. (1978-1979) 517-544.

[24] See. *Computer Fraud and Abuse Act*, 18 U.S.C. 1029 (1984).

[25] BARRY J. HUREWITZ AND ALLEN M. LO: Computer-Related Crimes. *American Criminal Law Review*, vol. 30. no. 3 (Annual Survey of White Collar Crime). (1993) 495-522.

Moreover, the concept of computer crime is also evolving. It has expanded with the development of the Internet. Computer crime or computer-related crime was defined as those crimes that use or target computer networks.[26] The Department of Justice of the United States also holds that computer crimes are interchangeably referred to as "computer-related crimes," "cybercrimes," and "network crimes."[27] The concept's expansion makes *computer crime* still great vitality and applicability today in academic research and official reports. For example, the Annual Survey of White Collar Crime, published every year since 1992 on the American Criminal Law Review, still uses the term *computer crime* to describe the annual situation of cybercrime.[28]

While it is technically possible to use the term computer crime to refer to all forms of cybercrime, this part argues that this approach is arguably out of date. At the heart of the term computer crime is still, literally, the computer. It is not indicative of the evolution of information network technology.

In today's world, the percentage of people who use computers to access the Internet is declining. People access the Internet in a variety of ways due to the popularity of mobile terminals. Additionally, Internet access via mobile devices, such as smartphones, has gradually become the mainstream.[29] Thus, without further explanation, this computer-centric term does not make an intuitive connection to the Internet. Moreover, the term computer crime conveys a view of cybercrime; that is, cybercrime is still object-based.

1.2.2 High-technology Crime

---

[26] CAROLINE FEHR, CHRISTINE LICALZI AND THOMAS OATES: Computer Crimes. *American Criminal Law Review*, vol. 53. no. 4 (Annual Survey of White Collar Crime). (2016) 977-1026.

[27] OFFICE OF LEGAL EDUCATION: *Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section, Criminal Division*. U.S. Department of Justice, 16 November 2021, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

[28] The most recent survey was in 2021. Please refer to: MATTHEW LARSON, ETHAN CANTOR, GABRIELLE CARON, ALESSANDRA LOPEZ AND DUNCAN WEALS: Computer Crimes. *American Criminal Law Review*, vol. 58. no. 3 (Annual Survey of White Collar Crime). (2021) 611-670.

[29] For example, in China, more and more people primarily use smartphones to access the Internet instead of the PCs. As of the end of June 2018, the proportion of Chinese netizens using mobile phones to access the Internet was 98.3%, 0.8 percentage point more than the end of 2017; the proportion of Chinese netizens using desktops and laptops to access the Internet was 48.9% and 34.5% respectively, decreasing 4.1 and 1.3 percentage points respectively from the end of 2017; and the proportion of Chinese netizens using TV to access the Internet was 29.7%, an increase of 1.5 percentage points from the end of 2017. [See. CHINA INTERNET NETWORK INFORMATION CENTER(CNNIC): *The 42nd Statistical Report on Internet Development in China*. China Internet Network Information Center (CNNIC), 1 October 2018, http://www.cnnic.com.cn/IDR/ReportDownloads/201911/P020191111253821210706 6.pdf]

"The world continues to change and does so more rapidly than ever before. These rapid changes are driven by high technology based on the microprocessor, which is the engine for all high-technology devices."[30] Accordingly, high-technology crimes involve using high-technology devices, such as computers, telephones, credit card machines, and any other device, including microprocessors, in its commission.[31] High-technology crime is a term that abstracts the technical characteristics of cybercrime as a generalization of a series of abuses of information network technology.

Supporters of the term High-technology Crime said, *High-technology Crime* or *Technocrime*, as a concept, "acknowledges the multi-dimensional qualities of the phenomena under investigation" and "embraces the interpretive and reactive elements of such offenses."[32] "Delineating clearly between *Technocrime* and other forms of crime seems to hinge on interpretation more so than any particular characteristics inherent in criminal acts or actors themselves."[33] Opponents of the term High-technology Crime said there was no need for an independent classification of high-technology crimes. The so-called high-technology crime is just a new form of traditional crime using technology.[34] This part argues that though desirable is it to apply the term *high-technology crime* to describe cybercrime, it also has some shortcomings.

First, on the surface, high technology does not necessarily represent information network technology. In other words, misusing information network technology is only one kind of high-technology crime. In China, for example, misuse of gene-editing technology could constitute an illegal practice of medicine.[35] When the term high-technology crime is

---

[30] GERALD L. KOVACICH AND ANDY JONES: *High-Technology Crime Investigator's Handbook: Establishing and Managing a High-Technology Crime Prevention Program*. Oxford, Elsevier, 2006. 2nd edition

[31] ROBERT MOORE, 2015, p. 2.

[32] KEVIN F. STEINMETZ AND MATT R. NOBLES: Introduction. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 1-10.

[33] KEVIN F. STEINMETZ AND MATT R. NOBLES, 2018. p. 6.

[34] "Technocrime does not exist. It is a figment of our imaginations. It is simply a convenient way to refer to a set of concepts, practices, frames and knowledges shaping the ways in which we understand matters having to do with the impact of technology on crime, criminals, and our reactions to crime – and vice versa: since crime, criminals and reactions also transform technology." [See. STEPHANE LEMAN-LANGLOIS: Introduction: Technocrime. In: STEPHANE LEMAN-LANGLOIS (ed): *Technocrime: Technology, Crime, and Social Control*. Devon, UK, Willan Publishing, 2008. 1-13.]

[35] PAN WANG, SISI XIAO AND YING ZHOU: *A verdict was pronounced in the "Gene Edited Baby" case. He Jiankui and other three defendants were held criminally responsible*. Xinhua Net, 16 November 2021, http://www.xinhuanet.com/2019-12/30/c_1125403802.htm

used to refer to cybercrime, it is inevitable to add that it is technology in the field of computers or information networks.

Second, using the term high-technology crime to describe cybercrime implies a controversial perception that the information network technology used by cybercriminals is always high. However, this is not the case. According to the *UNODC's Comprehensive Study on Cybercrime*, perpetrators often do not use complex information technology or sophisticated knowledge to engage in cybercrime because the Internet is already awash with relatively sophisticated malware programs that can be downloaded and used for free or at low cost.[36] For example, online fraud. Criminals use social software on the Internet to find targets and commit fraud. It is challenging to identify criminals using high technology to engage in online fraud because people's perceptions of high technology constantly evolve.

In addition, if high-technology crime only represents cybercrime, there is discriminatory prejudice. Can't innovations and advances in other technologies, except in the field of information networks, be considered high technology? The answer is no.

However, it must be noted that coining the term "high-technology crime" to refer to cybercrime represents an intellectual leap forward. In comparison to computer crime, this demonstrates that scholars have begun to pay attention to cybercrime's characteristics. This concern also reflects a shift in the focus of academic research on cybercrime away from superficial analysis and toward more in-depth analysis.

1.1.3 Cybercrime

Look up the word "Cyber" in the dictionary. It means relating to or involving computers or computer networks.[37] "Cyber" initially emerged from "cybernetics" and was envisioned studying feedback and control mechanisms within systems.[38] In the early days, the word "cyber" had no specific association with computer systems. This connection was established with the rise of the personal computer and technology subculture. In 1983, Bruce Bethke published the science fiction novel Cyberpunk, which co-opted the term Cyber. Then, throughout the 1980s and 1990s, the prefix "cyber" became a popular way to describe

[36] STEVEN MALBY, ROBYN MACE, ANIKA HOLTERHOF, CAMERON BROWN, STEFAN KASCHERUS AND EVA IGNATUSCHTSCHENKO (UNODC): *Comprehensive Study on Cybercrime (Draft)*. Vienna, United Nations Office on Drugs and Crime, 2013, p. 39.

[37] MERRIAM-WEBSTER DICTIONARY: *Definition of Cyber*. Merriam-Webster Dictionary, 15 November 2021, https://www.merriam-webster.com/dictionary/cyber

[38] NORBERT WIENER: *Cybernetics: Or Control and Communication in the Animal and the Machine*. New York, John Wiley & Sons, 1948.

anything digital, for instance, cyberspace and cybercrime.[39] Meanwhile, with the development of computer science technologies and the improvement of the Internet, the term computer crime could not cover all the circumstances in the new crimes—for example, the emergence of the mobile phone. So, it came to the "cybercrime" era.

It is worth mentioning that the use of the term cyberspace in the field of law and criminology is epoch-making. It marks scholars' recognition that Internet development has broken the territorial boundaries of the current legal system.[40] The Internet makes people worldwide closely connected and co-existing in a new space built on information network technology, namely Internet internationalization.[41] This new space, cyberspace, requires new rules different from traditional laws and regulations to govern the real problems that exist in or are associated with this space. From this point of view, cybercrime can be understood as a crime in cyberspace. Cybercrime governance is not only dependent on cyberspace governance but also an essential part of cyberspace governance.

Compared with the terms mentioned above, *computer crime* and *high-technology crime*, the advantages of the term *cybercrime* are that: it comprehensively considers the current development of computer technology and information technology and their impact on the production and life of human society. It is not limited to a specific object or technology, but the entire information network world as a virtual space independent of the physical world. Its name itself expresses the spatial characteristics of crime, and scholars also advocate this interpretive definition.

However, there are drawbacks to the term cybercrime. Some scholars criticize that the term cybercrime is too broad to accurately describe criminal behavior characteristics due to the ambiguity of the word cyber.[42] In other words, all incidents that occur in cyberspace or have minor connections with computers or the Internet may involve cybercrimes. This criticism is reasonable. Indeed, the term "cyber" is rife with ambiguity in terms of its scope. When an academic term contains this ambiguity, researchers are inevitably perplexed about the scope of the term's research. That is, as long as there is a cyber-related violation, it is

[39] KEVIN F. STEINMETZ AND MATT R. NOBLES, 2018. p. 3.

[40] DAVID R. JOHNSON AND DAVID POST: Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, vol. 48. no. 5. (1995) 1367-1402.

[41] HABIL ZOLTÁN NAGY AND DÁVID TÓTH: Computer Related Economic Crimes in Hungary. *Journal of Eastern-European Criminal Law*, vol. 2015. no. 2. (2015) 165-174.

[42] KEVIN F. STEINMETZ AND MATT R. NOBLES, 2018. p. 4.

considered a cybercrime, and in this era of the Internet of Things[43], all crimes could arguably be considered a cybercrime. As a result, the significance of distinguishing independent research from cybercrime is not immediately apparent.

Nevertheless, it is critical to understand that if the term "cybercrime" is used to describe a phenomenon, it reflects the fundamental characteristics of that behavior. Concerning the specific behavior, that is a separate subject, namely the morphology of cybercrime. According to this, this part argues that cybercrime terminology ranges from computer crime to high-technology crime to cybercrime, and that these terms reflect the evolution of people's understanding of cybercrime from a focus on specific objects to a focus on intrinsic technical characteristics to a summary of cybercrime's spatial characteristics.

1.2 Defining Cybercrime

The definition of cybercrime should be divided into two parts to understand itself. One is "cyber," and the other is "crime." In criminal law, crime is a norm or set of norms backed up by the deterrence of the criminal sanctions.[44] A crime must be an act or omission. Then here comes the question, what kind of action could be criminalized? What if a person criticizes the government in his blog very intensively? Should this act be criminalized?

There was a classification that distinguished the behaviors into normal ones and deviance.[45] Deviance is any violation of social norms, values, and expectations. It does not have a fixed meaning; it morphs in different environments and contexts. For example, homosexuality was deviance or even a crime before the 1960s in England and Wales. However, it has not been deviance or crime anymore, and gay couples can get married in England legally. The extension of the deviance is nonidentical, let alone the crimes. It could

[43] "The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction." [See. ALEXANDER S. GILLIS. *What is the internet of things (IoT)?* TechTarget, 11 March 2022, https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT] "At the 2005 World Summit on the Information Society, the International Telecommunication Union formally proposed the concept of "Internet of Things," proposing that the omnipresent era of "Internet of Things" communication is coming, and all objects in the world, from tires to toothbrushes, from houses to paper towels, can actively exchange information through the Internet." [See. HONGBO ZHU. *Internet of Things, Leaving no one behind in the Digital World* [物联网，开启万物互联时代]. Xinhua Net / People's Daily, 11 March 2022, http://www.xinhuanet.com/tech/2020-03/17/c_1125724344.htm]

[44] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS: *Criminology*. New York, Oxford University Press, 2017.

[45] ÉMILE DURKHEIM: *The Rules of Sociological Method*. New York, The Free Press, 1982. 1st American Edition

be found that all the crimes are deviant, but not all the deviance are law-related crimes. It is a necessary but not sufficient test. Some behaviors are deviant in some countries, but not in other countries. It is the same that some deviance is crimes in some countries, but not in other countries.

Then go back to cybercrime. If we want to get the meaning of crime therein, we should stand on two dimensions: the first is what kind of cyber behavior is deviance, and the second is what kind of cyber-deviance a crime is?

To answer the first question, we should bear in mind that it is a local thing sometimes. It depends on the different cultures, historical customs, and fundamental moral rules of a specialized area. Various societies have different values and practices. Keeping these norms is a way of understanding those who live in the same community, and it is challenging to change them in mind meanwhile. For instance, a man who is over twenty years old saw porn online. It might be a common occurrence in Europe as long as he did not watch child porn or at a public place or both, but it is deviant in China because obscene material is illegal and immoral.

To answer the second question, we should apply the "Harm Principle," i.e., crime is the deviance that jeopardizes others' interests, such as physical integrity, privacy, autonomy, and freedom from humiliation or degrading treatment.[46] Despite the detailed content of the harm principle, admitting that crime must be a harmful act is the same worldwide. However, in different countries, the definition of the harmful act is not identical. Then some acts might be deviant in some countries but a crime in others. For instance, three persons have sex in a hotel. Though secret is the place they had sex, willing are these three persons, and none of them engage in prostitution; it is still a crime in China, and their acts are treated as harmful for breaking down the public order and good morals.[47]

Based on the preceding two responses, we can conclude that, to comprehend the term "crime" in cybercrime fully, it is challenging to aggregate and summarize all relevant crimes contained in various conventions, treaties, or national legislation due to their dissimilar social origins. Therefore, if we continue to attempt to summarize the concept of cybercrime from a

[46] ANDREW VON HIRSCH AND NILS JAREBORG: Gauging Criminal Harm: A Living-Standard Analysis. *Oxford Journal of Legal Studies*, vol. 11. no. 1. (1991) 1-38.

[47] See. Article 301 of Criminal Law of People's Republic of China: Whoever takes a lead in assembling a crowd to engage in promiscuous activities or repeatedly participates in such activities is to be sentenced to not more than five years of fixed-term imprisonment, limited incarceration, or probation. [聚众进行淫乱活动的，对首要分子或者多次参加的，处五年以下有期徒刑、拘役或者管制。]

criminological perspective, we should first understand the distinction between the criminal law and criminology disciplines' definitions of crime or the nature of the crime.

The criteria for judging whether a particular type of conduct constitutes a crime in criminal law are relatively clear; that is, according to the principle of criminal law, a crime refers to an act that meets the constituent elements of a crime stipulated in the criminal law.[48] Criminal law mainly studies criminal law norms, aiming to reveal the normative meaning of crime and construct normative standards for the crime. Therefore, the criteria for judging whether a certain type of conduct constitutes a crime in criminal law by and large depend on, and are expressed in, the framework of criminal law norms and criminal law theory.[49] For instance, if a person uses the Internet to commit an act and satisfies the constituent elements of a crime under the criminal law, the person's behavior should be defined as a cybercrime.

Criminology's criteria for determining whether a particular act constitutes a crime are fairly complex. Along with criminal law, criminology should focus on general violations and deviances.[50] Criminology is primarily concerned with facts and phenomena in order to ascertain the factual significance of crimes and the factual standards for their expression. The criminological standard for determining whether a particular type of behavior constitutes a crime does not rely heavily on criminal law provisions or criminal law theory. It delves deeply into social facts.[51] In other words, the criminological concept of crime expresses precisely the social nature of criminal facts.

Different scholars held divergent views on the connotation of the social nature of criminal facts. Garofalo held the view that "while discarding the idea that morality is universal, it will nevertheless be possible for us to ascertain the identity of certain sentiments in a very wide field of human existence. It will also become clear to us that crime consists in acts which violate these same sentiments."[52] "The only sentiments which at the present day are of true importance for social morality are those termed altruistic, that is to say, such sentiments as have for their direct object the interest of others, although indirectly their exercise may redound to our own advantage. […] They may be reduced to two distinct types:

[48] See. MINGKAI ZHANG: *Essentials of Foreign Criminal Law* [外国刑法纲要]. Beijing, Law Press, 2020. 3rd edition. p. 43.

[49] See. XIAOHU ZHANG: *Criminology* [犯罪学]. Beijing, China Renmin University Press, 2017. 2nd edition. p.45

[50] See. WEI LI: *Fundamental Categories of Criminology* [犯罪学的基本范畴]. Beijing, Peking University Press, 2004. pp. 3-10.

[51] See. XIAOHU ZHANG, 2017, p. 46.

[52] BARON RAFFAELE GAROFALO: *Criminology*. Boston, Little, Brown, and Company, 1914. p. 15.

the sentiment of benevolence and the sentiment of justice."[53] Durkheim disagreed with Garofalo's definition of crime. He held that "the totality of beliefs and sentiments common to the average members of a society forms a determinate system with a life of its own. It can be termed the collective or common consciousness."[54] Except for the collective consciousness, "we can determine in no other way the nature of these sentiments nor define them in relation to their special purposes, for these purposes have varied infinitely and can vary again."[55] As a result, Durkheim stated that "an act is criminal when it offends the strong, well-defined states of the collective consciousness."[56] Ching-Yueh Yen, a Chinese scholar, defines crime from a cultural perspective. Yen believes that crime is a product of culture and evolves in response to cultural shifts. Crime develops in accordance with the collective's general culture and is a product of that culture.[57]

This section argues that Yen's proposal for a theory of cultural product is overbroad. Culture is a contentious and extremely rich concept in and of itself. According to Edward B. Taylor, "culture or civilization, taken in its wide ethnographic sense, is that complex whole which includes knowledge belief, art, morals, law, custom, and any other capabilities and habits acquired by man as a member of society."[58] Culture has such rich or ambiguous connotations. By incorporating it into the definition of crime, researchers will gain a more obscure understanding of the nature of the crime. Garofalo's theory of the same sentiments is also debatable. It is highly improbable or impossible that a universal sentiment of benevolence or justice transcends time and space and could be applied to all human beings from beginning to end. By contrast, Durkheim's theory of collective consciousness appears to be more plausible.

However, when these three theories are carefully examined, they all arguably point to a relatively identical target: something appears to exist in a society with commonalities; when an act violates this commonality, it can be defined as a crime. Prof. X. H. Zhang summed up this commonality as "the mainstream social norms established and advocated by a social state.

[53] BARON RAFFAELE GAROFALO, 1914, p. 19.

[54] ÉMILE DURKHEIM: *The Division of Labour in Society*. Houndmills, Basingstoke, Hampshire R021 2XS and London, The Macmillan Press, 1984. pp. 38-39.

[55] ÉMILE DURKHEIM, 1984, p. 34.

[56] ÉMILE DURKHEIM, 1984, p. 39.

[57] See. CHING-YUEH YEN: Crime in Relations to Social Change in China [中国的犯罪问题与社会变迁的关系]. Beijing, The Commercial Press, 2019.

[58] EDWARD BURNETT TYLOR: The Science of Culture. In: EDWARD BURNETT TYLOR (ed): *Primitive Culture: Researches into the Development of Mythology, Philosophy, Religion, Art, and Custom*. Cambridge, Cambridge University Press, 2010. 1-22.

Furthermore, what is hidden behind this mainstream social norm is the common interest of the vast majority of people in a society."[59] On top of this view, this section further summarizes it as common social values. On this basis, this part argues that an act is a crime from a criminological perspective should be regarded as a violation of common social values.

In his book *Theory of Legislation*, Jeremy Bentham put forward a comprehensive perspective of crime analysis, integrating 'what should be' and 'what is,' legislation and judiciary, substance and form.[60] In criminal law and criminology, we could find a variety of foci on whether a particular behavior constitutes a crime, based on Bentham's perspective and the preceding discussion. The judgment standard of criminal law[61] is: Formally, a crime is an act that meets the constituent elements of the criminal law; Substantially, a crime is an act with serious harm (A criminal act should meet the constituent elements of serious harm stipulated in the criminal law. In other words, the crime should have a significant seriousness or harm.[62]) The criterion of criminology is: Formally, crime is an act that violates the mainstream social norms established and advocated by society; Substantially, a crime is an act that seriously violates the common interests of the vast majority of people (common social values) in a society. By comparing the different judgment standards of criminal law and criminology, we can find a common element of judgment between the two; that is, they both emphasize that a certain behavior must cause a certain degree of harm. A crime should cause either *de jure* harm or *de facto* harm. Individually, harm in the normative sense is not allowed by law (or norms), while harm in the factual sense is not allowed by common social values. Of course, laws (or norms) and common social values are not absolutely separated, and there is an intersection between them. Considering that this dissertation's research on cybercrime is based on China's legislative and judicial practice, it inevitably discusses specific laws and regulations (norms). Therefore, this part adopts an eclectic angle to the definition of crime. That is, crime is a harmful behavior. It pursues improper interests (or profits). Such interests (or profits) are neither permitted by law nor common social values.

Following the definition of crime, this section attempts to incorporate it into defining cybercrime. This dissertation discussed three cybercrime terminologies in the preceding

[59] See. XIAOHU ZHANG, 2017, p. 46-48.

[60] See. JEREMY BENTHAM: *Theory of Legislation*. London, Trübner & Company, 1871.

[61] See. MINGKAI ZHANG: *Criminal Law* [刑法学]. Beijing, Law Press, 2021. 6th edition.

[62] See. Article 13 of Criminal Law of the People's Republic of China: "[H]owever, if the circumstances are clearly minor and the harm is not great, they are not to be deemed crimes." [但是，情节显著轻微危害不大的，不认为是犯罪]

section. From the introduction and analysis, it is not difficult to deduce that three terminologies represent three fundamental characteristics of cybercrime. The first is to rely on specific objects. While this object has evolved from computer to mobile terminal, the fundamental component is data and its online transportation.[63] The second strategy is to rely on technologies. While not all of these technologies are high-tech, they are generally advanced.[64] The third is the feature of cyber-spatialization. Cyber-spatialization implies that cybercrime is more of a crime in cyberspace, although some cybercrime does occur at the boundary between cyberspace and the physical world, as discussed in Section III of Chapter IV of this dissertation.

Cyberspace is teeming with data and information. Different subjects possess varying amounts of information in such a space. Their disparate sources of information may influence people to behave differently.[65] Additionally, when the amount of information possessed by various subjects varies, information asymmetry occurs. Asymmetric information (or information asymmetry) is a theoretical concept in economics. Its mission is to study market institutions and behavior, and in 2001, it was awarded the Nobel Prize in Economics.[66] Three researchers laid the groundwork for this theory in the 1970s: George Akerlof, Michael Spence, and Joseph Stiglitz. A fundamental tenet of asymmetric information (information asymmetry) theory is that sellers in a market have more information than buyers, affecting the transactions.[67] This section discusses cybercrime in terms of information asymmetry and argues, based on the fundamental proposition of information asymmetry theory, that the amount of information possessed by different subjects in cyberspace is also variable. This information asymmetry can be seen in cybercrime, where the offender might possess greater

[63] See. ISABELLE MAIGNAN AND BRYAN A. LUKAS: The Nature and Social Uses of the Internet: A Qualitative Investigation. *The Journal of Consumer Affairs*, vol. 31. no. 2. (1997) 355.

[64] See. LESLIE DAIGLE: On the Nature of the Internet. *Global commission on internet governance, paper series*, No. 7. Centre for International Governance Innovation and Chatham House, March 2015, https://www.cigionline.org/static/documents/gcig_paper_no7.pdf (The Technical Nature of the Internet, pp. 2-4.)

[65] See. LAURI AURONEN: *Asymmetric Information: Theory and Applications*. Tu-91.167 Seminar of Strategy and International Business at Helsinki University of Technology, Citeseer, 2003. 1-35.

[66] See. *Popular Information*, NobelPrize.org., 13 March 2022, https://www.nobelprize.org/prizes/economic-sciences/2001/popular-information/

[67] See. GEORGE A. AKERLOF: The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, vol. 84. no. 3. (1970) 488-500; SEAN ROSS: *Theory of Asymmetric Information*, Investopedia, 13 March 2022, https://www.investopedia.com/ask/answers/042415/what-theory-asymmetric-information-economics.asp

information resources[68], technical support[69], and/or a dominant position than the victim. Additionally, increased information resources and technical support in the hands of actors might be highly dependent on their dominant position, such as Internet companies' dominant position over their users.[70] When perpetrators take advantage of this information asymmetry, cybercrime might occur. In other words, when a perpetrator engaged in cybercrime, they were almost certainly taking advantage of cyberspace's information asymmetry.

It's time to make a summary. Through the above discussion, this section argues that: cybercrime is a harmful deviant behavior taken for procuring improper interests forbidden by law and/or common social values, by the feature of the data and online transportation thereof, which abuse the advanced technologies and/or the information asymmetries that get from positional advantages.

2. MORPHOLOGY OF CYBERCRIME

[68] "Consider the case of telecom fraud. In China, telecom fraudsters can typically obtain a large amount of personal information about citizens through illegal means. They then employ this information to commit fraud in accordance with a pre-written 'fixed script.'" See. XINING POLICE (XINING MUNICIPAL BUREAU OF PUBLIC SECURITY OF QINGHAI PROVINCE OF CHINA): *Common Telecom Fraud Routines Are All in These 10 Pictures!* [常见的电信诈骗套路，全在这 10 张图里!], thepaper.cn, 12 March 2022, https://m.thepaper.cn/newsDetail_forward_2840882

[69] "Technical support refers to the fact that criminals typically possess some relatively advanced Internet technologies that enable them to commit cybercrime more effectively than victims. This advanced technology is not truly cutting-edge. Rather than that, unless these technologies are specifically learned, they are not commonly used by the average Internet user or do not fall under the category of technologies that can be used in daily Internet use—for example, intelligent algorithms, Virtual Private Network services, and web crawlers." See. e.g., USMAN MAIMAITI AND WUMAIER ABUDUMIJITI: Artificial Intelligence Algorithm Personal Information Utilization Criminal Regulations and Personal Information Security Criminal Law Protection: From New Rights to New Legal Interests [人工智能算法个人信息利用刑法规制与个人信息安全刑法保护——从新型权利转向新型法益谈起]. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)* [重庆邮电大学学报(社会科学版)], vol. 34. no. 1. (2022) 48-60; YUQIANG WU: The Qualitative Analysis of the Behavior of Network "Crossing-the-Wall" Tools in Illegal Sales [非法销售网络"翻墙"工具行为的定性分析]. 2019 3rd International Seminar on Education, Management and Social Sciences (ISEMSS 2019). *Advances in Social Science, Education and Humanities Research*, vol. 345, 2019. 62-66; YUNFENG TONG: Research on the Regulation Limit of Cyber Crawler Behavior in Big Data Age [大数据时代网络爬虫行为刑法规制限度研究]. *Journal of Dalian University of Technology (Social Science)* [大连理工大学学报(社会科学版)], vol. 43. no. 2. (2022) 88-97.

[70] "Some websites such as information and online communities frequently pop-up windows to recommend apps when users browse the web, require downloading the app to view the full text, and not be able to read comments without the app, which hinders users from using the web to browse information and infringes on the legitimate rights and interests of users, and the masses react strongly." See. *Ministry of Industry and Information Technology: Internet Companies Are Not Allowed to Automatically or Forcefully Download Apps without User Consent* [工信部：互联网企业未经用户同意不得自动或强制下载 app], 3 March 2022, http://www.stdaily.com/index/kejixinwen/202203/23f191e515894989875494886f4a9883.shtml

The preceding section of this dissertation focused primarily on two points. Subsection 1.1 details the evolution of cybercrime's three terminologies. Subsection 1.2 defines cybercrime in terms of the three characteristics summarized above, as well as criminological perspectives on the nature of the crime. To aid in the development of a comprehensive understanding of cybercrime, this section will examine the morphology of cybercrime.

Morphology, as defined by the Merriam-Webster dictionary, mainly includes four meanings. The first meaning is based on biology. It is "a branch of biology that deals with the form and structure of animals and plants" or "the form and structure of an organism or any of its parts." The second meaning is based on linguistics. It is "a study and description of word formation in language" or "the system of word-forming elements and processes in a language." The third meaning is based on geology. It is "the external structure of rocks in relation to the development of erosional forms or topographic features." The fourth meaning is the general meaning of the word morphology, i.e., it is "a study of structure or form" or synonyms of "Structure/Form."[71] This section, titled Morphology of Cybercrime, focuses primarily on the fourth meaning. That is, this section's content is primarily concerned with the structure/form of cybercrime. This section will mainly discuss the various types of cybercrime. In summary, the previous section answered what cybercrime is in general, and this section will primarily address the question of what type of conduct constitutes cybercrime, i.e., the form/structure of cybercrime.

It is worth mentioning that this section is not under the title of the Structure/Form of Cybercrime, but the Morphology of Cybercrime. It is mainly because this section will not only introduce the structure/form of cybercrime but will also supplement some studies of the structure/form of cybercrime. These supplements will be mainly based on the Chinese context.

2.1 Morphology of Cybercrime in General

2.1.1 The Method of Particularization or Generalization

The morphology of cybercrime, in short, is the study of the composition or manifestation of cybercrime. This section argues that it mainly contains two methodologies. The first is the method of particularization. The second is the method of generalization. According to the theory of criminology or the current criminal law, the so-called method of

[71] See. *Morphology*, Merriam-Webster, 14 March 2022, https://www.merriam-webster.com/dictionary/morphology#note-1; *What Is Morphology?* All About Linguistics, 14 March 2022, https://all-about-linguistics.group.shef.ac.uk/branches-of-linguistics/morphology/what-is-morphology/

particularization refers to the exhaustion of all the specific behaviors that may constitute or have been cybercrime. The so-called method of generalization is to classify and summarize various types of cybercrimes currently existing based on existing criminal law and criminology theories and reveal the essential characteristics of specific types of cybercrimes in a typified form.

The advantage of the method of particularization is that it is relatively clear and explicit. In particular, adopting such a method in legal documents can reflect various types of cybercrime more clearly and help law enforcement and judicial departments make a more accurate judgment. However, the method of particularization also has its drawbacks. One of the most immediate flaws is that it is impossible to encapsulate all acts of cybercrime in one legal instrument, neither technically nor from the current state of development. At the moment, the Internet has permeated all spheres of social production and life, having a profound effect on them. Koops summarizes the Internet's seven megatrends. One of them is that the Internet is rapidly affecting or has already become the backbone of everything. The Datafication[72] of Everything is one of its manifestations.[73] They mean that all criminal acts against any aspect of physical society may be classified as cybercrime to some extent. On the other hand, information network technology is evolving at a breakneck pace. Correspondingly, the criminal methods of cybercrime are also constantly escalating.[74] The contradiction between the emerging new forms of cybercrime and the relatively lagging criminal legislation seems irreconcilable when only the method of particularization is adopted.

The advantage of the generalization method is that it is founded on an analysis and classification of cybercrime under current criminal law, in conjunction with criminological theory, and it summarizes cybercrime behavior according to a predetermined standard. In comparison to the method of particularization, it is more inclusive and open, reflecting the shared characteristics of a particular type of cybercrime. When implemented at the legislative level, it focuses on the legislature's responsibility to ensure that, in addition to clearly

[72] Datafication is a contemporary technological trend that involves the computerization of many aspects of our lives and the transformation of this data into new forms of value. See. ULISES A. MEJIAS AND NICK COULDRY: Datafication. *Internet Policy Review*, vol. 8. no. 4. (2019) 1-10; JATHAN SADOWSKI: When Data Is Capital: Datafication, Accumulation, and Extraction. *Big Data & Society*, vol. 6. no. 1. (2019) 1-12.

[73] BERT-JAAP KOOPS: Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. In: BABAK AKHGAR AND BEN BREWSTER (eds): *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Switzerland, Springer, 2016. 3-16.

[74] THOMAS J. HOLT AND ADAM M. BOSSLER: *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. London and New York, Routledge, 2016, pp. 2-5.

stipulating the specific behaviors of existing cybercrimes, sufficient legislative or interpretation space is left to accommodate evolving and innovative cybercriminal practices. However, the generalization method also has some room for discussion. The first concern is with classification criteria. Cybercrime can be classified using a variety of different classification criteria. (The following paragraphs will discuss this section of the content.) In academic research, it is feasible and encouraged to discuss cybercrime according to different criteria. In legislation and judicial practice, however, this approach is somewhat inappropriate. One of the straightforward questions is which criteria should be used. The second is a discretionary matter. Assuming a particular criterion is adopted, determining whether emerging behavior meets the standard (whether it constitutes a cybercrime or what type of cybercrime it constitutes) is left to law enforcement or judicial authorities' discretion. Additionally, this discretionary authority has the potential to be abused.

2.1.2 Examples of the Method of Generalization

The preceding section discussed two approaches to studying the morphology of cybercrime and their relative merits and demerits in legislative and judicial practice. This section begins the writing by introducing and analyzing the generalization classification of cybercrime. This subsection will not go into detail about various cybercriminal acts. The following subsection will discuss specific cybercrime behavior by combining China's criminal legislation and criminal law theory.

Several official institutions and academics have attempted to classify and discuss cybercrime in order to gain a better understanding of its morphology. The following are the official representative classifications:

First is the morphological classification of the U.S. Department of Justice. The U.S. Department of Justice defines cybercrime from the perspective of computer crime and gives its classification: (1) the computer as the target (by spreading viruses, launching a denial-of-service [DoS] attack, or launching an attack on a website); (2) the computer as a weapon (using a computer to commit traditional crimes such as identity theft, illegal gambling, or online pornography); (3) the computer used as an accessory or a device containing data incidental to the crime (using a computer as a method to maintain records on illegal or stolen information).[75]

[75] "In fact, the DOJ had not made these statements very clearly. According to the *Computer Crime: Criminal Justice Resource Manual (Second Edition)* published by the National Institute of Justice of the U.S.

The second is the morphological classification in the Budapest Convention. The Budapest Convention refers to the Convention on Cybercrime opened by the Council of Europe in Budapest on 23 November 2001. It entered into force on 1 July 2004. Chapter II, Section 1, Articles 2 to 13 of the Budapest Convention classifies cybercrime into four categories: (1) Offences against the confidentiality, integrity and availability of computer data and systems (They included Illegal access, Illegal interception, Data interference, System interference, and Misuse of devices); (2) Computer-related offences (Computer-related forgery and Computer-related fraud); (3) Content-related offences (Offences related to child pornography); (4) Offences related to infringements of copyrights and related rights.[76]

The third is the morphological classification from the United Nations Office on Drugs and Crime (UNODC). The UNODC's morphological classification of cybercrime is roughly the same as that in the Budapest Convention. However, UNODC, based on the morphological classification of the Budapest Convention, further divides cybercrime into the following categories: (1) Cyber-dependent offenses. They require an ICT infrastructure and are often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure, for example, the cyber-takeover of a power-plant by an organized crime group; and taking a website offline by overloading it with data, for example, a DDOS attack; (2) Cyber-enabled offenses. They can occur offline but can also be facilitated by ICT. They typically include online frauds, purchases of drugs online and online money

---

Department of Justice in 1989, the Manual, in the section on classification of computer crimes, according to Article 1030, Chapter 47, Title 18 of the US Criminal Code, only explicitly summarized the main four types of computer crimes: (1) The introduction of fraudulent records or data into a computer system; (2) Unauthorized use of computer-related facilities; (3) The alteration or destruction of information or files; (4) The stealing, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data. However, the *Computer Crime* section of the *Annual Survey of White Collar Crime*, published in the *American Criminal Law Review* for more than three decades, continues to cite the aforementioned Manual as a reference for defining and classifying cybercrime. Also, *Computer Crime* section summarized the three categories of cybercrime (the ones listed in this paragraph). In addition, Joshua B. Hill and Nancy E. Marion, in Chapter 3 of their monograph, argued that the three classifications of computer crime in this paragraph come from the US Department of Justice. To sum up, this paper believes that this classification method has certain credibility from the US Department of Justice." See. NATIONAL INSTITUTE OF JUSTICE OF U.S. DEPARTMENT OF JUSTICE: *Computer Crime: Criminal Justice Resource Manual (Second Edition)*, August 1989, https://files.eric.ed.gov/fulltext/ED332671.pdf; CAROLINE FEHR, CHRISTINE LICALZI AND THOMAS OATES: Computer Crimes. *American Criminal Law Review*, vol. 53. no. 4 (Annual Survey of White Collar Crime). (2016) 977-1026; JOSHUA B. HILL AND NANCY E. MARION: *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. California, Praeger: ABC-CLIO, LLC, 2016.

[76] See. COUNCIL OF EUROPE: *Convention on Cybercrime*. European Treaty Series-*No. 185*, Budapest, 23. XI. 2001.

laundering; (3) Online child sexual exploitation and abuse. It includes abuse on the clear internet, darknet forums, and the exploitation of self-created imagery via extortion.[77]

The representative morphological classifications from academics are as follows:

Eoghan Casey divides cybercrime into three main categories, all of which revolve around the computer: (1) The computer as a tool of crime. In this case, the computer is used to facilitate criminal activity. Without the computer being turned on and used in the commission of the act, the crime cannot be committed; (2) The computer as the focal point of a crime. In this case, the computer is the intended target of criminal activity and is not necessarily used in the commission of the act; (3) The computer as a repository of evidence. That is, the criminals kept the evidence on a computer.[78]

Eoghan Casey's classification method is valuable. Based on Casey's classification of computer crimes, some scholars summarize cybercrime as "computer-mediated activities that are illegal," and propose a dichotomy. That is, Cybercrime consists of (1) computer-assisted crimes (those crimes that predated the Internet, but which take on a new life in cyberspace, such as fraud, theft, money laundering, sexual harassment, hate speech, pornography) and (2) computer-focused crimes (those crimes that have emerged in tandem with the establishment of the Internet and could not exist apart from it, such as hacking, viral attacks, website defacement).[79]

This dichotomy is expanded into a trichotomy. Some other scholars divided cybercrime into three categories: (1) the computer or computer network is the target of crime, for example, hacking; (2) the computer or computer network is a tool to commit a traditional crime, such as theft or fraud; (3) the computer or Internet plays as an incident in committing crimes.[80] This trichotomy is largely consistent with the aforementioned morphological classification of the U.S. Department of Justice.

Majid Yar believes that the above-mentioned dichotomy or trichotomy may be "rather

---

[77] *Cybercrime: Global Programme on Cybercrime*, United Nations Office on Drugs and Crime, 15 March 2022, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

[78] See. EOGHAN CASEY: *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. New York, Academic Press, 2000; ROBERT MOORE, 2015.

[79] See. STEVEN FURNELL: *Cybercrime: Vandalizing the Information Society*. London, Addison-Wesley, 2001; PETER LILLEY: *Hacked, Attacked and Abused: Digital Crime Exposed*. London, Kogan Page Business Books, 2003; MAJID YAR: *Cybercrime and Society*. New Delhi, Sage, 2013. 2nd edition.

[80] See. SUSAN W. BRENNER: Nanocrime? *University of Illinois Journal of Law, Technology & Policy*, vol. 2011. no. 1. (2010) 1-74; JONATHAN CLOUGH: Cybercrime. *Commonwealth Law Bulletin*, vol. 37. no. 4. (2011) 671-680.

limited for criminological purposes, as it focused on the role played by the technology at the expense of the relationships between offenders and their targets or victims."[81]

Considering this, David S. Wall utilized existing categories drawn from criminal law into which their cyber-counterparts can be placed and sub-divided cybercrime into four established legal categories[82]: (1) Cyber-trespass (refers to the act of crossing invisible, yet established, boundaries of ownership in an online environment, such as hacking and malware); (2) Cyber-deception and theft (encompasses all ways that individuals may illegally acquire information or materials online, such as cyber-fraud and the theft of intellectual property via digital piracy); (3) Cyber-porn and obscenity (represents the entire range of sexual expression possible online. In addition, cyber-porn and obscenity include the problem of child pornography[83]); (4) Cyber-violence (refers to the opportunity afforded by technology to create, distribute or solicit access to injurious, hurtful, or dangerous materials, such as cyberbullying of juveniles, cyberstalking of adults, and hate speech against special groups).[84]

David S. Wall also applied a generational approach to distinguish cybercrime into three generations to date[85]: The first generation is low-end cybercrime, which refers to traditional crimes committed with the aid of computers. The second generation is hybrid cybercrime. It retained the characteristics of traditional crimes but was facilitated by computer networks to the point where the scale and scope began to differ significantly. The third generation is high-end cybercrime, which concerns crimes targeted at computers or computer networks themselves. Bert-Jaap Koops believes that a fourth generation of

[81] MAJID YAR, 2013. p. 22.

[82] See. DAVID S. WALL: Crime and the Internet. In: DAVID S. WALL (ed): *Crime and the Internet*. London, Routledge, 2001. 1-17.

[83] See. KEITH F. DURKIN: Misuse of the Internet by Pedophiles: Implications for Law Enforcement and Probation Practice. *Federal Probation*, vol. 61. no. 3. (1997) 14-18; KEITH F. DURKIN AND CLIFTON D. BRYANT: Propagandizing Pederasty: A Thematic Analysis of the on-Line Exculpatory Accounts of Unrepentant Pedophiles. *Deviant Behavior*, vol. 20. no. 2. (1999) 103-127; PHILIP JENKINS: *Beyond Tolerance: Child Pornography on the Internet*. New York, New York University Press, 2001; TONY KRONE: A Typology of Online Child Pornography Offending. *Trends and Issues in Crime and Criminal Justice / Australian Institute of Criminology*, no. 279. (2004) 1-6.

[84] See. MATT R. NOBLES, BRADFORD W. REYNS, KATHLEEN A. FOX AND BONNIE S. FISHER: Protection against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization among a National Sample. *Justice Quarterly*, vol. 31. no. 6. (2014) 986-1014; SAMEER HINDUJA AND JUSTIN W. PATCHIN: *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. California, Corwin, 2015. 2nd edition; THOMAS J. HOLT AND ADAM M. BOSSLER, 2016, pp. 10-15.

[85] DAVID S. WALL: *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, Polity, 2007.

cybercrime should be added to David S. Wall's generational approach. The fourth generation of cybercrime may be vacillating between completely virtual crime (committed in virtual worlds) and ambient crime (target at Ambient Intelligence, or what is now usually referred to as the Internet of Things).[86]

In general, the morphological classification of cybercrime discussed previously focuses on either the role technology played in cybercrime or the conduct of cybercrime regulated in current criminal law. Another morphological classification, on the other hand, is distinct from the previous two approaches. It focuses on cybercrime's intended victim or on the object or target of cybercrime. According to this view, cybercrime can be classified into the following categories: (1) cybercrime against the person (for example, cyberbullying, cyberstalking, and online harassment); (2) cybercrime against property (for example, hacking, malware, cyber-fraud, and intellectual property piracy); (3) cybercrime against morality (for example, cyber-pornography and child pornography); and (4) cybercrime against the state (for example, cyber-terrorism and espionage of official secrets).[87] Or， (1) cybercrime against people; (2) cybercrime against the property; (3) cybercrime against the government. [88]

Each of the morphological classifications presented and discussed in this section, whether official or academic, has its own set of criteria. The various forms of morphological classification of cybercrime stand on different emphases. All of them are valuable to some extent. This subsection introduces and discusses these morphological classifications of cybercrime in order to provide a macro perspective on it. Simultaneously, this subsection focuses on the method of generalization, making few references to specific cybercriminal acts. The following subsection will discuss them in detail with reference to specific provisions of Chinese criminal law.

2.2 MORPHOLOGY OF CYBERCRIME IN CHINA

This subsection will primarily demonstrate how cybercrime is a crime in China, based on the specific cybercrime provisions in the People's Republic of China's current criminal

[86] The reference to fourth-generation cybercrime is still the one originally proposed by David S. Wall. However, Bert-Jaap Koops extends the scope of fourth-generation cybercrime, from the Internet of Things to the Internet of People. According to Koop: "Internet of People is looming on the horizon, driven by an increasing use of implants on or inside the body." The Internet of People should be related to the objects with networking capabilities that people implant in the body or the electronic devices with networking capabilities that are worn outside the body. See. BERT-JAAP KOOPS, 2016, p. 7.

[87] MAJID YAR, 2013. p. 23.

[88] JOSHUA B. HILL AND NANCY E. MARION, 2016, pp. 50-70; PAVAN DUGGAL: *Artificial Intelligence, Cybercrimes & Cyberlaw*. Independently Published, 2018.

law. Additionally, this section will conduct a brief doctrinal analysis of the crimes involved in light of Chinese criminal law's general theory.[89]

The provisions on cybercrime in China's Criminal Law are mainly concentrated in Section 1, Crimes of Disrupting Public Order [妨害社会管理秩序罪], of Chapter VI, Crimes of Disrupting Social Administration Order [扰乱公共秩序罪], of the Criminal Law. Specifically, Articles 285, 286, 286(I), 287, 287(I), and 287(II) of the Chinese Criminal Law。

Article 287 is a provision that serves as a guideline for addressing the use of computers to commit crimes.[90] It provides that the use of computers as a criminal tool or means of committing traditional crimes shall be punished in accordance with the Chinese Criminal Law's corresponding provisions. In other words, article 287 considers certain types of cybercrime to be traditional crimes committed via information network technologies such as the Internet and computers. For example, under the provisions of this article, the use of the Internet to commit fraud (cyber fraud) shall be prosecuted and punished in accordance with the Chinese Criminal Law's provisions on fraud (i.e., Article 266, Crime of Fraud [诈骗罪]), and the use of the Internet to distribute obscene materials shall be prosecuted and punished in accordance with the Criminal Law's corresponding provisions on disseminating obscene materials (i.e., Article 364, Crime of Disseminating Obscene Materials [传播淫秽物品罪]).

Article 285 defines four types of cybercrime: Crime of unauthorized intrusion into computer information systems [非法侵入计算机信息系统罪], Crime of unauthorized acquisition of data from computer information systems [非法获取计算机信息系统数据罪],

[89] The constitutive elements of the crimes discussed in this subsection are largely based on Prof. Gao Mingxuan and Prof. Ma Kechang's criminal law textbook. Generally, in China, the ideas in this textbook are regarded as general views of criminal law theory. In this textbook, the constitutive elements of crime usually include four parts: the object of the crime [犯罪客体], the objective aspect of the crime [犯罪客观方面], the subject [犯罪主体], and the subjective aspect of the crime [犯罪主观方面]. The object of crime refers to the social values protected by criminal law and violated by criminal acts. The objective aspect of the crime is the socially harmful behavior stipulated by the criminal law and should be punished by criminal punishment, and the result of this behavior that causes or may cause harm to the society (which is approximately similar to *Actus reus*). The subject of crime refers to the natural person and unit that commits acts that endanger society and should bear criminal responsibility according to the criminal law. The subjective aspect of crime is the psychological attitude of the perpetrator to the crime committed by himself and the result of the crime (which is approximately similar to *Mens rea*). See. MINGXUAN GAO AND KECHANG MA: *Criminal Law* [刑法学]. Beijing, Peking University Press, 2022. 10th edition.

[90] See. Article 287 of Criminal Law of People's Republic of China: Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law [利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚].

Crime of unauthorized controlling computer information systems [非法控制计算机信息系统罪], Crime of providing programs or tools for unauthorized intrusion or control of computer information systems [提供侵入、非法控制计算机信息系的程序、工具罪]. Article 286 defines the Crime of vandalizing computer information systems [破坏计算机信息系统罪]. Article 286(I) defines the Crime of Refusing to Fulfill the Obligation of Information Network Security Administration [拒不履行信息网络安全管理义务罪]. Article 287(I) defines the Crime of illegal utilization of information network technology [非法利用信息网络罪]. Article 287(II) defines the Crime of provision of assistance to conduct the cyber-criminal activity [帮助信息网络犯罪活动罪].

Crime of unauthorized intrusion into computer information systems. This crime is established in Article 285, paragraph 1. The subject of the crime of this crime may be either a natural person with full capacity for criminal responsibility who has reached the age of 16[91] or a unit [单位].[92] (In the discussion of specific cybercrime in China later in this subsection, in the case of the subject of the crime, unless there are special provisions, it is the same as this crime. In the subsequent introduction of the crime, if the subject of the crime is not mentioned, please refer to it here.) The objective aspects of this crime are as follows: (1) violates state regulations[93] and (2) intrudes into computer systems with information concerning state affairs, construction of defense facilities, and sophisticated science and technology. The subjective aspect of this crime is intention.

Crime of unauthorized acquisition of data from computer information systems. This crime is established in Article 285, paragraph 2. The objective aspects of this crime are as follows: (1) violates state regulations, (2) intrudes into a computer information system other

[91] See. Article 17 of Criminal Law of People's Republic of China: Where a person who has attained the age of 16 commits a crime, the person shall assume criminal liability [已满十六周岁的人犯罪，应当负刑事责任].

[92] According to the provisions of the Chinese Criminal Law, units refer to as companies, enterprises, institutions, organs and groups. It is similar to a legal person. See. Article 30 of Criminal Law of People's Republic of China: A company, enterprise, institution, organization, or group which commits an act endangering society that is considered a crime under the law shall bear criminal responsibility [公司、企业、事业单位、机关、团体实施的危害社会的行为，法律规定为单位犯罪的，应当负刑事责任].

[93] See. Article 96 of Criminal Law of People's Republic of China: The phrase "violating state stipulations/regulations" in this law refers to violation of laws and decisions formulated by the National People's Congress or the National People's Congress Standing Committee; and administrative measures prescribed in administrative ordinance and regulations formulated by the State Council; as well as decisions and decrees the State Council promulgated [本法所称违反国家规定，是指违反全国人民代表大会及其常务委员会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令].

than that prescribed in paragraph 1 of Article 285 or (3) uses other technical means, (4) to obtain the data stored, processed or transmitted in the said computer information system (5) with serious circumstances. The subjective aspect of this crime is intention.

Crime of unauthorized controlling computer information systems. This crime is established in paragraph 2 of Article 285 as well. The objective aspects of this crime are as follows: (1) violates state regulations, (2) exercises illegal control over a computer information system other than that prescribed in paragraph 1 of Article 285 (3) with serious circumstances. The subjective aspect of this crime is intention.

Crime of providing programs or tools for unauthorized intrusion or control of computer information systems. This crime is defined in paragraph 3 of Article 285. The objective aspects of this crime are as follows: (1) provides special programs or tools specially used for intruding into or illegally controlling computer information systems, or (2) knows that any other person is committing the criminal act of intruding into or illegally controlling a computer information system and still provides programs or tools for such a person, (3) with serious circumstances. It is critical to note that this crime does not require that the computer information system that is the target of this crime be the one defined in paragraph 1 of Article 285. In other words, providing a program or instrument to a person attempting to hack into or gain illegal control of a commercial or civilian computer information system also constitutes this crime. Furthermore, although the subjective aspect of this crime is the intention, it also requires the perpetrator to "know," which refers to a psychological state in which the perpetrator is aware of others' illegal or criminal acts but still provides assistance.

Crime of vandalizing computer information systems. The objective aspect of this crime has three manifestations: (1) violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences (focus on the operation of the system); (2) violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences (focus on data and programs in the system); (3) deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences (focus on Malware). The subjective aspect of this crime is intention.

Crime of Refusing to Fulfill the Obligation of Information Network Security Administration. In addition to requiring it to be a natural person with full capacity for

criminal responsibility who has reached the age of 16 or a unit, the subject of this crime must also be an information network service provider with an obligation to manage information network security as prescribed in any law and administrative regulation. The objective aspects of this crime are as follows: (1) fails to perform the information network security management obligation as prescribed in any law or administrative regulation, (2) refuses to make corrections after being ordered by the regulatory authority to take corrective measures, and causes any of the following consequences: (a) causing the spread of a large amount of illegal information; (b) causing the leakage of users' information, with serious consequences; (c) causing the loss of criminal case evidence, with serious circumstances; (d) any other serious circumstance. The subjective aspect of this crime is intention.[94]

Crime of illegal utilization of information network technology. The objective aspects of this crime are as follows: (1) establishes a website or a communication group mainly for committing fraud, teaching on how to commit a crime, producing or selling any prohibited or controlled article, or committing any other illegal or criminal activity; (2) issues any information on the production or sale of drugs, guns, obscene materials, or any other prohibited or controlled article or any other illegal or criminal conduct; (3) issues any information for committing fraud or any other illegal or criminal activity. To put it simply, the objective aspects of this crime include three aspects: one is to set up a website or communication group for the purpose of committing the crime; the second is to publish illegal and criminal information (it emphasizes the illegality and criminality of the information content); and the third is to publish information for the commission of the crime

[94] In China, the subjective component of this crime is controversial. There are different perspectives on negligence, recklessness, intention, and vague guilt. This part holds that the subjective aspect of this crime is intention. The following are the reasons: To begin, whenever an expression such as "refusal to do it" appears in the provisions of other crimes in the Chinese Criminal Law, the subjective aspect of the crime is almost always intention. Second, the "obligations" imposed by this crime are of a professional nature. Because the perpetrator is capable of conducting business with such professionalism, he cannot be unaware of the criminal consequences of his actions. The third is that one of the elements constituting this crime is disobedience of a supervisory authority's order. The perpetrator's refusal to execute after receiving the order must be deliberate unless the perpetrator is truly incapable of carrying out the order. Of course, the perpetrator's inability to carry out the order does not constitute this crime. See. WANGYUAN XIE: On the Crime of Refusing to Fulfill the Obligation of Information Network Security Administration [论拒不执行信息网络安全管理义务罪]. *China Legal Science* [中国法学], no. 2. (2017) 238-255; BINGZHI ZHAO AND QIWEI ZHAN: Formation of Crime Regarding Nonfulfillment of Secure and Manage Obligation on Information System and Network [论拒不执行信息网络安全管理义务罪的罪过形式]. *Guizhou Social Sciences* [贵州社会科学], vol. 360. no. 12. (2019) 61-67; LING QIU: Analysis on Crime of Refusing to Perform the Obligation of Information Network Security Management [拒不履行信息网络安全管理义务罪探析]. *Law Science Magazine* [法学杂志], vol. 41. no. 4. (2020) 64-71.

(it does not emphasize the illegality and criminality of the information itself, but emphasizes the illegality and criminality of the purpose of publishing the information). The subjective aspect of this crime is intention.

Crime of provision of assistance to conduct the cyber-criminal activity. The objective aspects of this crime are as follows: (1) provides Internet access, server custody, network storage, communication transmission or any other technical support, or (2) provides advertising, payment settlement or any other assistance for the crime, and (3) with serious circumstances. The subjective aspect of this crime is intention. Additionally, it requires the offender of this crime to be aware of attempts by others to commit crimes through the use of information networks.

To sum up, morphologies of cybercrime in China are manifested as an indicative clause and eight specific cybercrimes. Briefly speaking, the criminal legislation on cybercrime in China is centered on information network technology. China also criminalized the conduct of aiding cybercrime as an independent cybercrime. Meanwhile, China stipulates the criminal liability of units (corporate liability, or criminal liability of legal person) for committing cybercrime. It's worth noting that China's approach to information network technology as a core reflects ideas that are strikingly similar to those expressed in the U.S. Department of Justice's classification of cybercrime (i.e., focus on technology). Therefore, the following parts of this dissertation will mainly consider and cite cases or regulations in the U.S. as reference to discuss some common issues within cybercrime.

3. CRIMINOLOGICAL THEORETICAL UNDERSTANDING OF CYBERCRIME: BASED ON THE SOCIOLOGICAL APPROACHES IN CRIMINOLOGY

Despite every piece of evidence pointing to cybercrime as a huge area of need for preventative efforts, criminological researchers are indeed finding it difficult to "keep up." One particular shortcoming of criminological cybercrime research is that theoretical studies seeking why people commit cybercrime are scarce.[95] However, when we make a brief review of the existing research on cybercrime, it is not difficult to find that the existing research has not been carried out independently without the guidance of a certain theory. Every mature or published empirical research on cybercrime is based on the framework of a certain

[95] JOHN H. BOMAN IV AND ADRIENNE FRENG: Differential Association Theory, Social Learning Theory, and Technocrime. In: KEVIN F. STEINMETZ and MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. p. 55.

criminological theory. These countless studies will not be introduced here. Their researchers obtain theoretical expectations from the theory, and through operationalization, they convert the basic propositions in the theoretical framework into testable hypotheses to carry out research. However, although researchers rely on theoretical guidance to carry out empirical research, few published works systematically sort out the criminological theories on which empirical research on cybercrime relies.[96] In other words, the existing criminology research on cybercrime or criminal law research is mostly an in-depth discussion of a certain theory. Therefore, after studying cybercrime and reading much literature, this article tried to summarize or comb the criminological theories applied in the current empirical research on cybercrime. It is also the starting point of this article.

Among the numerous criminology theories, this article chooses the theories in the branch of modern sociological approaches in criminology as the focus of the research. Modern sociological approaches in criminology refer to the general term for theories and viewpoints put forward in the 20th century using sociological theories and methods to study crime problems.[97] The basic viewpoints of Modern sociological approaches in criminology include: (1) Criminal behavior is a social phenomenon, which is caused by criminogenic social conditions, in which unreasonable social systems, social structures, and social processes play a particularly important role in promoting it; (2) The pattern of criminal behavior is closely related to the offender's socio-economic status, race, gender, and age; (3) Social changes are related to criminal behavior. Changes in norms, values, systems and structures affect how individuals and groups commit crimes; (4) *The development of technology and its impact on social systems play an important role in the occurrence of crime*; (5) The interaction within intergroup and individuals has an important impact on the occurrence of crime.[98]

Modern sociological approaches of criminology are an umbrella term for a disparate range of the applications of sociological theories within the scope of criminological research. Many theories are constituting these new academic schools compared with the criminological research before the 20th century. Some scholars attempted to classify or categorize it.[99]

---

[96] e.g., See. KEVIN F. STEINMETZ AND MATT R. NOBLES: *Technocrime and Criminological Theory*. New York, Routledge, 2018.

[97] ZONGXIAN WU: *History of Criminology in the West* [西方犯罪学史]. Beijing, Press of People's Public Security University of China, 2010. 2nd edition, p. 975.

[98] ZONGXIAN WU, 2010. pp. 977-78.

[99] See. e.g., Travis Hirschi categorized existed sociological approaches in criminology into three parts: (1) Strain

Among them, the more representative classification of modern sociological approaches in criminology comes from Larry J. Siegel. He divides modern sociological approaches in criminology into four categories[100]:

(1) Social Structure Theory. It consists of four intersecting branches: Cultural Deviance Theory, *Strain Theory*, Subcultural Theory, and Social-Ecological Theory.

(2) Social Process Theory. The sub-theories that constitute the framework of social process theory mainly include *Social Learning Theory* [including *Differential Association Theory*], Control Theory, and Social Reaction Theory [or Label Theory].

(3) Social Conflict Theory. The connotation and extension of the social conflict theory are relatively rich. Many theoretical groups have been derived from the concept of social conflict, including Conflict Theory, *Marxist Criminology* [or *Critical/Radical Criminology*], *Postmodern Criminology*, *Feminist Criminology*, etc.

(4) Integrated Theory. It includes Social Development Theory and Interaction Theory, etc.

After a preliminary introduction to the basic content of sociological approaches in criminology, the reason for choosing sociological approaches in criminology as the theme of this article is clear. On the one hand, as mentioned above, technological innovation and progress can impact crime is one of the basic propositions of sociological approaches in criminology, and show that sociological approaches in criminology are naturally adaptable to explain cybercrime caused by Internet technological innovation and development. On the

---

Theory or Motivational Theory; (2) Control Theory or Bond Theory; (3) Cultural Deviance Theory. This kind of theory also could be termed as Cultural Conflict, Cultural Transmission, Subcultural, and Differential Association. [TRAVIS HIRSCHI: *Causes of Delinquency*. New York, Routledge, 2002.] Ronald L. Akers divides sociological theories into four categories: (1) Social Disorganization and Anomie Theory; (2) Conflict Theory; (3) Labeling and Stigmatization Theory; (4) Social Control Theory. [RONALD L. AKERS: *Deviant Behavior: A Social Learning Approach*. Belmont, California, Wadsworth, 1973.] Gwynn Netter's classification: (1) Subcultural Theory; (2) Structural Theory; (3) Symbolic Interaction Theory; (4) Control Theory. [GWYNN NETTLER: *Explaining Crime*. New York, McGraw-Hill, 1974.] William V. Pelfrey also categorized sociological approaches in criminology into four parts. However, his classification was on the basis of the work of Travis Hirschi. In Pelfrey's classification, the first three categories were the same with the Hirschi's trichotomy. The fourth one is Symbolic Interactionist Theory. Pelfrey hold the viewpoint that Symbolic Interactionist Theory constitutes the underpinning premises of many criminological theories. The Differential Association Theory and Label Theory are two main theories constitutes the Symbolic Interactionist Theory, and they might be the most influential theory in the cluster of criminological theories. [WILLIAM V. PELFREY: *The Evolution of Criminology*. Cincinnati, Ohio, Anderson, 1980.]

[100] See. LARRY J. SIEGEL: *Criminology: Theories, Patterns, and Typologies*. Boston, Massachusetts, CENGAGE Learning, 2016. 13th edition. pp. 187-342. [Chapter 6-9]

other hand, as Professor Wu Zongxian stated, the theoretical popularity of sociological approaches in criminology and the popularity and abundance of theoretical results indicate that the mainstream of criminology in the 20th century is sociological approaches in criminology.[101] Therefore, choosing this theoretical framework to explain cybercrime can easily find the existing published results as support.

This part will follow Larry J. Siegel's classification and pay more attention to the Strain Theory in Social Structure Theory, the Differential Association Theory/Social Learning Theory in Social Process Theory, Radical Criminology, Postmodern Criminology, and Critical Feminist Theory in Social Conflict Theory. The following part will first introduce the underpinning propositions of these theoretical frameworks; then discuss the application thereof to cybercrime explanation and understanding; at last, this article will give some comments on these applications to cybercrime. In the end, this article will summarize these theoretical frameworks and propose advice for future research.

3.1 SOCIAL STRUCTURE THEORY: STRAIN THEORY

Briefly, Strain Theory holds that crime and delinquency are the products of depression, anxiety, and anger the people in society experience when they cannot achieve social or economic success. Strain Theory began with the work of Robert K. Merton[102] and then further developed and enriched by Messner and Rosenfeld's Institutional Anomie Theory[103], Passas' Global Anomie Theory[104], and Robert Agnew's General Strain Theory[105]. For concision, this part will mainly focus on Merton's Strain Theory and Agnew's General Strain Theory.

3.1.1 Merton's Strain Theory

In the early twentieth century, Robert K. Merton put forward the strain theory to study and analyze deviant/criminal behavior. This theory is developed with the core viewpoint of

[101] ZONGXIAN WU, 2010. p. 977.

[102] ROBERT K. MERTON: Social Structure and Anomie. *American Sociological Review*, vol. 3. no. 5. (1938) 672-682.

[103] STEVEN F. MESSNER AND RICHARD ROSENFELD: *Crime and the American Dream*. Belmont, California, Wadsworth, 2013. 5th edition.

[104] *See*. NIKOS PASSAS: Anomie and Corporate Deviance. *Contemporary Crises*, vol. 14. no. 2. (1990) 157-178. NIKOS PASSAS: Global Anomie, Dysnomie, and Economic Crime: Hidden Consequences of Neoliberalism and Globalization in Russia and Around the World. *Social Justice*, vol. 27. no. 2. (2000) 16-44.

[105] ROBERT AGNEW: Foundation for a General Strain Theory of Crime and Delinquency. *Criminology*, vol. 30. no. 1. (1992) 47-88.

"anomie" in the research of Émile Durkheim[106], and it focuses on the logical deduction of social anomie that creates strain and illicit behavior on individuals.

The core point of Merton's strain theory is that universal goals set by social culture have a profound impact on people's behavior in society. The biased or wrong goals caused by social-cultural anomie can cause strain in society. This strain will, in turn, cause people in society to have different behavioral responses.[107]

Merton summed up different behavioral response adaptations or adjustments into five forms: Conformity, Innovation, Ritualism, Retreatism, and Rebellion.[108] Among them, conformity is the most common way of behavior, that is, to comply with the overall value of society and work hard to achieve social goals and expectations. Retreatism refers to not accepting the overall value goal of society but adopting an evasive attitude toward the world, and there is no deviance or crime in behavior. Ritualism means that, on the one hand, it does not accept the overall value goals under social and cultural anomie; on the other hand, it forms a formal response to this situation, showing a perfunctory attitude. Innovation refers to not recognizing the existing social value goals and adopting non-conventional and universally recognized means to achieve this goal. Although it shows a kind of helplessness, it still uses certain behaviors to achieve the value goals and social expectations. Rebellion is similar to innovation. They both question or disagree with the existing value goals of society to varying degrees. However, rebellion exhibits two ways of behavior. One is revolutionarily breaking the existing value goals and social expectations and constructing a new goal and value system; the other is adopting deviant or criminal conducts to achieve goals.

Merton further elaborated on "anomie" and "anomia and strain" in subsequent research. Anomie is "a breakdown of social standards governing behavior resulting in little social cohesion." In contrast, anomia is "the anomic state of individual" arising from the uncertainty that "others will be in rough accord with standards jointly regarded as legitimate."[109] In other words, anomie manifested in a general strain caused by the deviant social value goal of the whole society, for example, regarding the pecuniary success or the

---

[106] *See*. ÉMILE DURKHEIM: *Suicide: A Study in Sociology*. London, Routledge, 1951. 2nd Edition; ÉMILE DURKHEIM: *The Division of Labour in Society*. Houndmills, Basingstoke, Hampshire R021 2XS and London, The Macmillan Press, 1984.

[107] KIMBERLY A. CHISM AND KEVIN F. STEINMETZ: Technocrime and Strain Theory. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 66-84.

[108] ROBERT K. MERTON, 1938. p. 678.

[109] ROBERT K. MERTON, 1964. p. 227.

monetary wealth as the only criterion of success for all social members. Anomia mainly expresses the individual's different responses to value goals and social expectations in social life. Although there are certain problems with the overall social value goal, everyone's views and reactions to this problem are different. Some people will adopt obedience or innovation to achieve it, while others will adopt a rebellious approach and commit crimes or deviant behavior to achieve the goal. On the other hand, it is a source of strain for one person, but it does not necessarily cause strain for another person—there is implied anomia.

Anomie is caused by the value goal of society as a whole. However, it can be divided into anomie of success and anomie of failure.[110] The anomie of failure could be easily understood: failure to achieve social value, which leads to personal tension. The strain felt by those who successfully realize the overall value goal of society is the anomie of success. On the one hand, the actual satisfaction of reaching the social value goal is lower than expected. On the other hand, perhaps, after achieving a certain social value goal, an individual has discovered a new and higher social culture based on existing achievements anticipation, and then the individual needs to struggle endlessly to achieve higher goals, which makes this type of people feel the strain.[111] In terms of successful anomie, those who can quickly achieve social value goals are more likely to feel tension than those who achieve their goals through long-term sustained efforts.

The series of adaptations arising from strain, as mentioned above, is divided into four categories. Among them, both the innovative and rebellious types have a great possibility of giving birth to deviant or criminal behavior. However, the social reality is cruel. Not only are the legal opportunities for realizing the overall value of the society unevenly distributed across all levels, but even the illegal opportunities are the same.[112] When a person has criminal motives, on the one hand, the door needs to experience the tension of anomie. On the other hand, it is also relatively critical. They also have to have the means available to commit crimes or deviant behaviors.

3.1.2 Agnew's General Strain Theory

Based on Merton's strain theory, Agnew proposed the General Strain Theory. Agnew believes that there are various sources of tension besides failing to meet the compulsory goals

[110] ROBERT K. MERTON, 1964. p. 220.

[111] KIMBERLY A. CHISM AND KEVIN F. STEINMETZ, 2018. p. 69.

[112] RICHARD A. CLOWARD AND LLOYD E. OHLIN: *Delinquency and Opportunity*. Chicago, Illinois, University of Chicago Press, 1960.

of social culture. Strain may stem from three aspects: (1) failure to achieve positive value goals; (2) removal of positive value effects; (3) introduction of negative effects.[113] The influence of strain on deviant and criminal behaviors is mediated by "negative emotions" This negativity includes various emotions that can adversely affect people's behavior, such as depression, tension, and anger.[114] Among them, anger is the emotion that deserves the most attention under the general tension theory.[115]

Agnew believes that there is a difference in strain. This difference is reflected in the different ways in which individuals encounter tension. The way an individual encounters tension can be divided into three independent forms: (a) experience, (b) anticipated, (c) vicarious strain. Experienced strain refers to the tension that directly affects the individual; the predicted tension is the pressure caused by anticipating that certain tension may or will happen; the alternative tension is the pressure that people feel when they witness the unfair treatment of other people. That is, the indirect pressure experienced through the suffering of others.

Agnew further divides strain into an objective and subjective one.[116] Objective strain is defined as an event or condition that most members of a given group do not like. The disgusting and stressful cognition of specific stimuli has a certain degree of universality. In other words, the general public hates a certain stimulus, and the general public feels pressure on a certain stimulus. This kind of universality, similar to reaching a consensus, makes this kind of target stimulus objective tension. The subjective stimulus is specific to the individual. In other words, what some people think of as stress is not stressful for others.

3.1.3 Application of Strain Theory on Understanding Cybercrime

Broth Merton's strain theory and Agnew's general strain theory have certain advantages and limitations in explaining cybercrimes.

Regarding the high incidence of cybercrimes of infringement of intellectual property rights, cyberpiracy is the result of a social/cultural disconnect between socially recognized means and goals. On the one hand, the infringer is in a general context of a consumer

[113] ROBERT AGNEW: Foundation for a General Strain Theory of Crime and Delinquency. *Criminology*, vol. 30. no. 1. (1992) 47-88.

[114] KIMBERLY A. CHISM AND KEVIN F. STEINMETZ, 2018. p. 70.

[115] ROBERT AGNEW, 1992.

[116] ROBERT AGNEW: Building on the Foundation of General Strain Theory: Specifying the Types of Strain Most Likely to Lead to Crime and Delinquency. *Journal of Crime and Delinquency*, vol. 38. no. 4. (2001) 319-361.

society.[117] This kind of social background promotes consumerism and stimulates people to pursue a full range of high consumer lifestyles to meet an assortment of psychological, emotional, and social needs[118]; on the other hand, people's actual economic conditions and capabilities cannot support this excessive consumerism, which will create strain for members of society. Under the influence of strain, social members' different behavioral adaptation patterns will inevitably lead to innovation or rebellion—inducing members to acquire the ability or content of consumption by illegal means.[119] In terms of digital content, the existing society promotes and encourages people to greedily consume intellectual property products, such as movies, music, online games, office software, etc. The anonymity and sharing characteristics of the Internet will inspire people to bypass the traditional business model recognized method-paid access and obtain digital content by other means deemed illegal under the existing legal system-free download and share.[120]

Another good example is the crime of online fraud as Majid Yar stated that "Diminished barriers to entry, Internet-facilitated anonymity, jurisdictional limitations on law enforcement, and las legal regimes internationally make online fraud from certain countries particularly appealing – including those in Eastern Europe, Sub-Saharan Africa, and Southeast Asia."[121] Internet technology plays two roles in cyber fraud.

The first role is the source of strain. Internet technology, especially the widespread popularity of social media, enables the rapid sharing and dissemination of certain social value goals and values, which is, of course, positive. However, social media, particularly short video platforms, can sometimes have a deleterious effect on the process of spreading values in China. On the short video platform, users upload their own works or retweet other's ones. Under normal circumstances, a short video will play for approximately ten seconds. The creators of short videos are very clear that the best way to increase data traffic to their account is to create as many stimuli as possible to capture users' attention within a limited amount of time.

According to Alfred Adler, the founder of individual psychology, when people are

[117] KEVIN F. STEINMETZ AND KENNETH D. TUNNELL: Under the Pixelated Jolly Roger: A Study of On-Line Pirates. *Deviant Behavior*, vol. 34. no. 1. (2013) 53-67.

[118] SAMEER HINDUJA: *Music Piracy and Crime Theory*. New York, LFB Scholarly Publishing, 2006. p. 130.

[119] STEFAN LARSSON, MÅNS SVENSSON AND MARCIN DE KAMINSKI: Online Piracy, Anonymity and Social Change: Innovation through Deviance. *Convergence*, vol. 19. no. 1. (2013) 95-114.

[120] STEFAN LARSSON, MÅNS SVENSSON AND MARCIN DE KAMINSKI, 2013. p. 108.

[121] KIMBERLY A. CHISM AND KEVIN F. STEINMETZ, 2018. p. 73; MAJID YAR AND KEVIN F. STEINMETZ: *Cybercrime and Society*. London, Sage, 2019. 3rd Edition.

psychologically or physically frustrated or feel inferior, they will compensate in other ways to alleviate their inferiority/anxiety.[122] Watching short videos on short video platforms only takes up fragmented time and is free. Simultaneously, the content on the short video platform provides viewers with intense stimulation and satisfaction in a short period of time. As a result, watching short videos appears to be the most cost-effective method of compensation available to Chinese people today. From the side, statistics from Quest Mobile in 2021 confirm this: the short video platform has 872 million monthly active users and an average monthly usage time of 42.6 hours (The data was collected from January to December in 2020). With the continued growth of short video users, the growth rate has slowed significantly, but people's per capita usage time for short videos continues to grow at a rapid clip. The short video industry's influence continues to grow.[123]

When commercial short video platforms are inundated with a large amount of content about a specific topic, the content must meet a wide range of needs and appeal to a wide range of audiences. In current China, short video platforms are flooded with content to show off pecuniary success, the fantasy of getting rich overnight, and various fragments of extravagant lives.[124] Short videos of showing off pecuniary success provide much rush, or stimulation, in a very short period of time, arousing various emotions of the audience, envy or jealousy.[125] This feature will make such short videos very easy to gain the favor of users and platforms. Specifically: (1) As far as viewers are concerned, according to the information cocoons theory (i.e., "communications universes in which we hear only what we choose and only what comforts and pleases us") proposed by Cass R. Sunstein, when viewers "liked" watching such videos, they will habitually watch more such videos under the guidance of interest.[126] (2) As far as creators are concerned, the audience's likes and demand for such videos will further fuel their enthusiasm for creating more such videos and uploading them on the platform. (3) As far as short video platform operators are concerned, when they find that

[122] See. ALFRED ADLER: *What Life Could Mean to You*. Business and Leadership Publishing, 2014.

[123] See. QUEST MOBILE: *Quest Mobile China Mobile Internet 2020 Annual Report (Part 2): Mobile Internet Industry Inventory* [Quest Mobile 中国移动互联网 2020 年度大报告(下篇):移动互联网行业盘点], Quest Mobile, 2 February 2021, https://www.questmobile.com.cn/research/report-new/143

[124] XINHUA NEWS: *Xinhua News criticizes the phenomenon of short video platform showing off wealth: this extravagant trend should be taken care of!* [新华社批短视频平台炫富现象: 这股奢靡之风该管管了], 21 October 2021, https://finance.sina.com.cn/china/2021-04-15/doc-ikmxzfmk7034255.shtml

[125] See. YING WANG: On Discussion of the Social Effects Caused by Wealth Flaunt Advertising [试论炫富广告引发的社会效应]. *Lanzhou Academic Journal* [兰州学刊], no. S1. (2008) 153-154.

[126] See, CASS R. SUNSTEIN: *Infotopia: How Many Minds Produce Knowledge*. New York, Oxford University Press, 2006. pp. 9-11.

such videos are very "hot," they use algorithms to describe user preferences and then push interest.[127] In other words, the short video platform intelligently pushes what users like to watch.

To sum up, in China, users will repeatedly experience short videos of showing off monetary success to some extent. And this looped repetitive experience can cause users, especially teenagers and young adults, to have the illusion that their peers have generally achieved great wealth and monetary success. At the same time, these high-profile rich people will be mistaken for successful people through deformed social value goals. When users compare their situation, they perceive themselves as a loser. Then, the strain arises.[128]

Moreover, members of modern Chinese society inevitably have to use online social platforms[129], which makes people have to become the audience of these contents, which is not a choice; and the upgrading of network technology has made these contents available at an unprecedented speed and breadth. The wanton spread in the society has caused widespread tension among members of society. Network technology and social network platforms have inevitably become a source of tension for the entire society.

The second role represents a convenient apparatus of behavioral adaptation. As the content related to wealth and success widely promoted on social networking platforms has caused general strain among members of the society, according to Merton's Strain Theory,

---

[127] See. FENGMING WEN AND XUEFANG XIE: The Operation Logic and Ethical Concerns of the Short Video Recommendation Algorithm: Based on the Actor Network Theory [短视频推荐算法的运行逻辑与伦理隐忧：基于行动者网络理论视角]. *Journal of Southwest Minzu University (Humanities and Social Science)* [西南民族大学学报(人文社会科学版)], vol. 43. no. 2. (2022) 160-169.

[128] See. JIANGUO JIANG: Wealth Flaunt on Internet: Spiritual Poverty and Lost Values [网络炫富:精神贫困与价值迷失]. *Modern Communication (Journal of Communication University of China)* [现代传播(中国传媒大学学报)], vol. 35. no. 2. (2013) 15-19.

[129] WeChat, QQ and DingTalk are now the three mainstream online social platforms in China. The number of daily active users of WeChat alone is as high as 1 billion. An ordinary Chinese day cannot leave WeChat. It has the function of instant messaging, social networking, and even online payment. The communication between people does not even use the traditional way of calling but uses WeChat or QQ internal video chat or voice chat. DingTalk, on the other hand, is a piece of software that specializes in serving enterprises. It has 500 million individual users and 17 million organizational users. These have created a common phenomenon in China. As long as people want to communicate with others, whether it is for work or life, they can not escape these three applications to a large extent because they are free (no extra costs other than data traffic), fast, and function-rich. See. *Tiktok Has 400 Million Daily Active Users, Wechat Has 1 Billion, and You May Not Think of Alipay's Number* [抖音日活 4 亿，微信 10 亿，支付宝日活可能你想不到], Tencent, 13 January 2020, https://xw.qq.com/amphtml/20200113A0S6V300; *Which Companies Are Using Ding Talk?* [哪些企业在用钉钉?], Ding Talk, 17 March 2022, https://www.dingtalk.com/qidian/help-detail-20288922.html

members of the society will adopt different behavioral adaptation models to achieve social value goals. The network's convenience, low cost, widespread, and anonymity have undoubtedly become a convenient apparatus to achieve goals. Members who adopt the innovative and conform adaptations can legally use Internet technology to obtain wealth, such as live webcasts and the provision of high-quality online content. However, due to capacity limitations, the propaganda content on social networking platforms spread more one-sided information---creators only emphasized wealth and success and ignored the methods of obtaining wealth and achieving success. In this context that only emphasizes consequentialism, people will only focus on realizing the goal and ignore the means to achieve the goal. In turn, members of society who adopt a rebellious behavior adaptation model will use the Internet to engage in fraud, gambling, and other illegal and criminal activities to obtain wealth and achieve social value goals. In reality, the threshold for cyber fraud is too low and does not require much technical support. Some groups specializing in cyber fraud have fixed patterns and "scripts" in fraud by which Internet technology is just a convenience s method.[130]

3.1.4 Comments

In summary, we can find that, in the final analysis, the deviation of social and cultural value goals has led to a large number of crimes. Network technology only amplifies these effects and becomes an important promoter of deviation goals and a convenient means of achieving goals by mistake. The strain theory has its advantages in explaining the phenomenon of the surge in cybercrime and the causes of cybercrime. At least it provides a new perspective for us to understand cybercrime. However, the strain theory has its limitations:

First, the core of supporting the strain theory is the anomie of social value goals, which causes general strain among members of society. How to measure whether a value goal is anomie is very important. When measuring objective tension, the solution of strain theory proponents is that most events or conditions in a given social group that do not like or feel tension can be considered.[131] Then, how to ensure that a given group selected in empirical research represent society's views as a whole? After all, proponents believe that

[130] YE QIAN: *Telecom fraud "scenario" has been renovated so quickly, users become "stunned birds"* [电信诈骗"剧本"翻新神速　用户成"惊弓之鸟"], Xinhua News, 21 October 2021, http://www.cac.gov.cn/2016-01/02/c_1117649793.htm

[131] ROBERT AGNEW, 2001. p. 320.

tension based on individual cognitive differences is subjective tension when defining subjective tension.[132] It is difficult for social survey research to achieve a full sample survey and analysis. Sampling is inevitable, so the rationality of sampling directly affects the authenticity and credibility of the results.[133] Errors at this stage will directly subvert the entire research process because judging whether the social and cultural value goals are out of standard is the logical prerequisite for all theory analyses.

Second, the strain theory's starting point and endpoints are the analysis and regulation of the macroscopic aspects of society. It takes a long time to adjust the social value goals established in the past because the time for people to establish Worldview, Philosophy of life , and Values are often very short, but the impact of the three intellections on people usually lasts for a long time. Therefore, correcting the social value goal to adjust the intellections of social members to alleviate strain is often intergenerational. Therefore, it is desirable to use tension theory to guide social policy and criminal justice in the long run. However, the strain theory does not seem to have short-term high efficiency and high returns in the face of the increasingly urgent need to combat cybercrime. In other words, when it comes to the social micro-level, the advantages of strain theory are not so obvious. Of course, every theory has its starting point for thinking. It is unfair to force the macro theory to be applied to the micro-level and use its discord as the object of criticism.

3.2 Social Process Theory: Differential Association Theory and Social Learning Theory

Social Process Theory, or called Social Interaction Theory, refers to micro-sociological theories. It looks at elements close to the individual and explains crime in terms of the immediate social situation an individual finds him-/herself in and how that impacts choices and behaviors. It focuses on small groups and individuals; and considers how people behave and interact, then creating their society.[134] There is an assortment of theories under the framework of Social Process Theory. However, this part will mainly discuss the Differential Association Theory and Social Learning Theory briefly for concision.

3.2.1 Differential Association Theory

[132] See. ROBERT AGNEW, 2001.

[133] SHUHUA LU: *Social Statistics* [社会统计学]. Beijing, Peking University Press, 2009. 4th edition, pp. 449-450.

[134] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS: *Criminology*. New York, Oxford University Press, 2017. pp. 379, 383.

It is generally believed that Edwin H. Sutherland proposed the Differential Association Theory in 1939 and expanded it in his 1949 publication.[135] The simplest interpretation of Differential Association Theory, which might be relatively improper, is that people's criminality can be affected by contact with different people or interactions with unspecified people or groups. Differential Association Theory can be summarized in this minimalist expression because the basic attribute of the theory is a learning theory.[136] In other words, the primary learning mechanism comes from persons referred to as "differential associates" or people that an actor associates with, in various capacities, that aid in constructing definitions favorable or unfavorable to the commission of a crime.[137]

The framework of Sutherland's Differential Association Theory includes arguably, once were seven, nine propositions:

(1) *Criminal Behavior is learned*;

(2) *The learning happens in interaction with other people*;

(3) *Most learning of criminal behavior occurs within close groups*. In the practice of research, researchers operationalized close groups of the differential associate as an actor's peers or friends[138] and treated friends or peers of an actor as focal differential associates[139];

(4) *The learning constituted by the know-how essential to offending, as well as the motives, drives, rationalizations, and attitudes necessary to commit a crime*;

(5) *The direction of motives and drives is learned from interpreting the norms/rules as being favorable or unfavorable*;

(6) *An actor turns to delinquency or offending is the result by definitions favorable to violation excessing that unfavorable*. Therefore, neutral is only in terms of differential associates themselves. Either criminal associates or anti-criminal ones could impact definitions of violation of the law. So, problematic is not differential associates but the "content" (people or groups) implicated in the differential associate;

(7) *Differential associates vary in modalities of association, i.e., frequency, duration,*

[135] JOHN H. BOMAN IV AND ADRIENNE FRENG, 2018. p. 56.

[136] EDWIN H. SUTHERLAND, DONALD R. CRESSEY AND DAVID F. LUCKENBILL: *Principles of Criminology*. Lanham, Maryland, General Hall 1992. 11th edition.

[137] JOHN H. BOMAN IV AND ADRIENNE FRENG, 2018. p. 56; ZONGXIAN WU, 2010. p. 921.

[138] DEREK A. KREAGER: Strangers in the Halls: Isolation and Delinquency in School Networks. *Social Forces*, vol. 83. no. 1. (2004) 351-390.

[139] JOHN H. BOMAN IV AND ADRIENNE FRENG, 2018. p. 57.

intensity, and priority. Frequency and duration are easy to understand, so that needs no more explanations. Priority refers to the early experience of a person. It stresses that early experience, whether delinquent or normal, could impact a person's mode of conduct in a relatively long time. Difficult is to give intensity a concise definition. It encompasses many factors, such as the fame of source of non-/criminal modeling and emotional reactions involved in associates.

(8) *Learning criminal behavior shares the same mechanism with that of any other general behavior*;

(9) *General needs and values cannot explain criminal conduct though expression/stratification does exist in criminal conduct. Cause noncriminal behavior necessitates general needs and values as well.* The practice of explaining crime confuses criminal behavior and noncriminal behavior with general needs and values, such as the principle of happiness, monetary success, frustration, and failure, etc.

3.2.2 Social Learning Theory

Social Learning Theory is a theory of learning process and social behavior which proposes that new behaviors can be acquired by observing and imitating others.[140] As a branch of behavioral theory, its development was based on the behavioral learning theory, prompted by John Watson, Clark Hull, and Burrhus Frederick Skinner.[141] In Social Learning Theory, human behaviors are learned by observational learning and learning by direct experience. Observational learning generally happens in home modeling, subcultural group modeling, and symbolic modeling; and is with the processes of attention, retention, reproduction, and motivation.[142] The aversive instigator, incentive instigator, modeling instigator, instructional instigator, and delusional instigator will arouse the particular behavioral pattern acquired in observational learning and learning by direct experience. After the first attempt of acquired behavior aroused by instigators above, the actor will keep those behavioral patterns by external reinforcement, vicarious reinforcement, and internal

[140] *See*. MARK KELLAND: *Social Learning Theory and Personality Development*. openstax CNX: Personality Theory in a Cultural Context, 23 October 2021 https://cnx.org/contents/lISyy6OT@1.1:oiev6HcT@1/Social-Learning-Theory-and-Personality-Development; ALERT BANDURA: *Social Learning Theory*. General Learning Process, 23 October 2021, https://web.archive.org/web/20131024214846/http://www.jku.at/org/content/e54521/e54528/e54529/e178059/Bandura_SocialLearningTheory_ger.pdf

[141] ZONGXIAN WU, 2010. p. 960.

[142] ALBERT BANDURA: Modeling Theory: Some Traditions, Trends, and Disputes. In: ROSS D. PARKE (ed): *Recent Trends in Social Learning Theory*. Academic Press, 1972. 35-61.

reinforcement.[143]

As a psychology theory, social learning theory has also produced tremendous inspiration for other non-psychological disciplines since its birth, including criminology. To resolve the issue of the unclear specification of how learning occurred[144] left by Sutherland's Differential Association Theory, Ronald Akers and Robert Burgess created a comprehensive theory of criminal behavior by integrating the principles of Social Learning Theory and Operant Conditioning, which could be seen as an extension of Differential Association Theory and known as the application of Social Learning Theory in Criminology.[145]

On the one hand, Social Learning Theory in Criminology directly applied Sutherland's definitions and differential association (and the modalities of association). It proposes that "interaction with differential associates who engage in deviance or crime will cause a person to form definitions favorable or unfavorable to deviance or crime."[146]

On the other hand, Social Learning Theory in Criminology "incorporates the concept of imitation from Skinner's research[147] to explain the learning process. It also adds the concept of differential reinforcement, which describes the process through which one's associations reinforce behavior (either deviant or not)."[148] As Burgess and Akers stated that "criminal behavior is learned in both social and nonsocial situations through combinations of direct reinforcement, vicarious reinforcement, explicit instruction, and observation."[149]

3.2.3 Application of Social Learning Theory on Understanding Cybercrime

As mentioned above, Social Learning Theory in criminology was developed as an extension of Differential Association Theory for rectifying the shortcomings and enriching

---

[143] JOAN E. GRUSEC: Social Learning Theory and Developmental Psychology: The Legacies of Robert Sears and Albert Bandura. *Developmental Psychology*, vol. 28. no. 5. (1992) 776-786.

[144] DONALD R. CRESSEY: Epidemiology and Individual Conduct: A Case from Criminology. *Pacific Sociological Review*, vol. 3. no. 2. (1960) 47-58.

[145] STEPHEN PFOHL: *Images of Deviance and Social Control: A Sociological Histor*y. New York, McGraw-Hill, 1994; ROBERT L. BURGESS AND RONALD L. AKERS: A Differential Association-Reinforcement Theory of Criminal Behavior. *Social Problems*, vol. 14. no. 2. (1966) 128-147.

[146] RONALD L. AKERS: *Social Learning and Social Structure: A General Theory of Crime and Deviance*. New York, Routledge, 2009.

[147] BURRHUS F. SKINNER: *Science and human behavior*. Oxford, England, Macmillan, 1953.

[148] JOHN H. BOMAN IV AND ADRIENNE FRENG, 2018. p. 58.

[149] MARK KELLAND: *Social Learning Theory and Personality Development*. openstax CNX: Personality Theory in a Cultural Context., 23 October 2021 https://cnx.org/contents/lISyy6OT@1.1:oiev6HcT@1/Social-Learning-Theory-and-Personality-Development;

and better functioning Sutherland's theory. Therefore, research examining one theory is necessarily relevant to the other.[150] So, though under the title of Social Learning Theory is this part, both Differential Association Theory and Social Learning Theory's application on understanding cybercrime will be briefly introduced and discussed here.

The earliest research on cybercrime using social learning theory can be traced back to William F. Skinner and Anne M. Fream's work in 1997. By analyzing a sample of college students and combining social learning theory, they found that individuals with high numbers of friends engaged in cyber deviance were heavily involved in piracy and hacking.[151]

George E. Higgins and David A. Makin's works showed that Differential Association and Definitions had a link with physical media software piracy when the piracy was for sharing software with a friend or when the piracy was for their interests by using a sample of college students.[152] George E. Higgins, Brian D. Fell, and Abby L. Wilson found that both the Self-control Theory and Social Learning Theory could come together to explain digital piracy. Social Learning Theory could partially mediate the effect of self-control on digital piracy by analyzing a non-random sample of 393 undergraduates.[153] Sameer Hinduja and Jason R. Ingram used a sample of approximately 2000 college students to identify the differential impact of offline and online peer influence on participation in music piracy under the framework of Social Learning Theory. After controlling for individuals' demographic characteristics and Internet capabilities, the real-life peers had the strongest effect. However, the online peers and online media sources also had significance in predicting music piracy participation.[154]

Robert G. Morris and Ashley G. Blackburn's research on computer hacking lend modest support to Social Learning Theory based on self-report data with the size of 600. However, in studying four forms of computer hacking, they found that the impact of social

---

[150] JOHN H. BOMAN IV AND ADRIENNE FRENG, 2018. p. 57.

[151] WILLIAM F. SKINNER AND ANNE M. FREAM: A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, vol. 34. no. 4. (1997) 495-518.

[152] GEORGE E. HIGGINS AND DAVID A. MAKIN: Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy? *Journal of Economic Crime Management*, vol. no. 2. (2004) 1-22; GEORGE E. HIGGINS AND DAVID A. MAKIN: Self-Control, Deviant Peers, and Software Piracy. *Psychological Reports*, vol. 95. no. 3. (2004) 921-931.

[153] GEORGE E. HIGGINS, BRIAN D. FELL AND ABBY L. WILSON: Digital Piracy: Assessing the Contributions of an Integrated Self-Control Theory and Social Learning Theory Using Structural Equation Modeling. *Criminal Justice Studies*, vol. 19. no. 1. (2006) 3-22.

[154] SAMEER HINDUJA AND JASON R. INGRAM: Social Learning Theory and Music Piracy: The Differential Role of Online and Offline Peer Influences. *Criminal Justice Studies*, vol. 22. no. 4. (2009) 405-420.

learning components may vary across the different forms of hacking.[155] Robert G. Morris' other work on understanding hacking based on a sample of university students and orchestrated Differential Association Theory, Neutralization Techniques[156], and Self-control Theory[157], revealed that Differential Association Theory and Neutralization Techniques were propitious to explain hacking but ineffective was Self-control Theory.[158] To summarize, hacking is a crime arguably based on hacker cultural groups. This kind of cybercrime is specific, and its criminal group is relatively close compared to other criminal groups. For example, there are generally some hacker technology forums for computer technology enthusiasts to exchange, study and discuss, and this will often develop into a crime. By contacting such groups, learning-related hacking techniques, or imitating the social image of hackers' transformative, rebellious, high-tech, and other social images, potential criminals' criminal motives and motivations are strengthened, and crimes are promoted. It is very consistent with the model construction of these two theories.

Theoretical examinations of Social Learning Theory and Differential Association Theory are relatively abundant, making these two theories popular in criminology study. However, with the increasing social learning theory research, some researchers turn to epistemology and methodology of social learning theory. Combined with the research on cybercrime or cyber deviance, they expanded the original theoretical framework, reconfigured the epistemological system of Social Learning theory and Differential Association Theory, summarized and progressed the methodological issues in the existing research.

Thomas J. Holt, George W. Burruss, and Adam M. Bossler applied structural equation modeling to evaluate the full social learning process. They found "social learning to be a second-order latent construct that explained a large variation in cyber deviance." Moreover,

---

[155] ROBERT G. MORRIS AND ASHLEY G. BLACKBURN: Cracking the Code: An Empirical Exploration of Social Learning Theory and Computer Crime. *Journal of Crime and Justice*, vol. 32. no. 1. (2009) 1-34.

[156] See. GRESHAM M. SYKES AND DAVID MATZA: Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, vol. 22. no. 6. (1957) 664-670.

[157] See. MICHAEL R. GOTTFREDSON AND TRAVIS HIRSCHI: *A General Theory of Crime*. Stanford, California, Stanford University Press, 1990.

[158] See. ROBERT G. MORRIS: Computer Hacking and the Techniques of Neutralization: An Empirical Assessment. In: THOMAS J. HOLT AND BERNADETTE H. SCHELL (eds): *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications.* Hershey, Pennsylvania, IGI Global, 2011. 1-17; also see. GEORGE W. BURRUSS, ADAM M. BOSSLER AND THOMAS J. HOLT: Assessing the Mediation of a Fuller Social Learning Model on Low Self-Control's Influence on Software Piracy. *Crime & Delinquency*, vol. 59. no. 8. (2013) 1157-1184.

the social learning process "mediated the effects of race and sex on cyber deviance."[159] Sameer Hinduja and Jason R. Ingram found that if conceptualize the intensity of Differential Association Theory as friendship quality, it is necessary to distinguish the friendship with terrestrial peers and hybrid and cyber peers cause the former carries a significantly different connotation than the former latter.[160] As for both theories' research methodology and epistemology, Travis C. Pratt et al. collected 133 studies related to cybercrime/cyber deviance and Social Learning Theory as the sample. Through the Meta-analysis, they assessed the core propositions specified by social learning theory.[161]

3.2.4 Comments

However, the outstanding advantages of these two theories in explaining some cybercrimes do not mean that these two theories are fully capable of explaining complex cybercrimes as a whole. Related research reflects that some problems in applying these two theories deserve to be considered and resolved.

In terms of research content, the core concepts of both theories involve association. The traditional association is offline and face-to-face. Cyberspace has changed this way of association, and three types of the association have emerged. One is a pure online association, netizens; the second is a pure offline association, the association in the terrestrial model; the third is a compound association, offline friends contact in the form of online. The relevance of these three forms of contact to induce criminal motives and strengthen or weaken criminal intentions has not been fully discussed in recent years using these two theories to study cybercrime.[162] In other words, there is a lack of hypothesis testing and parametric analysis based on theoretical conceptualization for the three forms of contact alienated by cyberspace.

In terms of research methods, there are at least two problems in cybercrime research using these two theories. One is that most of the existing research samples are cross-sectional analyses without establishing comprehensive panel data. It means that social learning has not been thoroughly tested, especially in the process of differential reinforcement. Second, almost

---

[159] THOMAS J. HOLT, GEORGE W. BURRUSS AND ADAM M. BOSSLER: Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. *Journal of Crime and Justice*, vol. 33. no. 2. (2010) 31-61.

[160] SAMEER HINDUJA AND JASON R. INGRAM, 2009.

[161] TRAVIS C. PRATT, FRANCIS T. CULLEN, CHRISTINE S. SELLERS, L. THOMAS WINFREE, TAMARA D. MADENSEN, LEAH E. DAIGLE, NOELLE E. FEARN AND JACINTA M. GAU: The Empirical Status of Social Learning Theory: A Meta-Analysis. *Justice Quarterly*, vol. 27. no. 6. (2010) 765-802.

[162] JOHN H. BOMAN IV AND ADRIENNE FRENG, 2018. pp. 61-62.

all studies on social learning theory and cybercrime use a non-random sample of college students, which makes the conclusions of these studies not universally applicable. Although George E. Higgins and David A. Makin argued, college students are most likely to engage in software piracy because they are young, educated, and have a deep understanding of computers.[163] However, the sample of students has the prerequisites for cybercrime. The mastery of computer technology, young, educated, and in-depth understanding of the team does not necessarily lead to such groups being more likely to commit crimes than other groups. For example, college students, especially Chinese students, must take primary legal education in the university. They all have a certain understanding of crime and illegality. According to the Social Learning Theory and Differential Association Theory model, college students are also likely to receive negative reinforcement (abandon the original criminal intent). Moreover, in the existing crime statistics, the educational background of criminals engaged in cybercrime is balanced, and the proportion of criminals with higher education is not significantly high compared to other criminals.[164]

3.3 Social Conflict Theory: Radical Criminology and Feminist Criminology

Social Conflict Theory is a sociological theory based on Marxism. The theory believes that the interaction between society members and classes is based on conflict rather than consensus. Karl Marx and Friedrich Engels believe that, according to the theory of social conflict, contradictions of interest and conflicts of scarce resources between various classes in society constitute the foundation of society.[165] Unfortunately, we live in a society flooded with economic, political, and social conflicts.[166] The social construction based on this social background reacts to social life, producing so-called *inequality*. The sub-theories that constitute the modern Social Conflict Theory in Criminology group derived from absorbing the concept of social conflict into crime research are quite rich.[167] For example, Radical and Feminist Criminology, which revolve around the research and reflection on *inequality*, constitute the main components of Social Conflict Theory in Criminology.

3.3.1 A Brief Introduction to Radical Criminology

[163] GEORGE E. HIGGINS AND DAVID A. MAKIN, 2004. p. 928.

[164] DAWEI SONG: Sentencing Disparity in China: A descriptive Research on Auxiliary Cybercrime Stipulated by Amendment IX of criminal law. *Iustum Aequum Salutare*, vol. XVII. no. 2. (2021) 209-239.

[165] KIMBERLY MOFFITT AND JEFFREY PERRY: *Social Conflict Theory in Sociology: Definition & Contributors*. Study.com, 26 October 2021 https://study.com/academy/lesson/social-conflict-theory-in-sociology-definition-lesson-quiz.html

[166] LARRY J. SIEGEL, 2016. pp. 271-272.

[167] See. Figure 8.1 *Branches of Social Conflict Theory*. in LARRY J. SIEGEL, 2016. p. 273.

When the focus shifted from the microscopic focus on general personal crimes or deviant behaviors and their characteristics to the inequality mentioned above between powerful and powerless people or classes, the basic framework and propositions of Radical Criminology were established. As Richard Quinney stated, criminal labels and definitions are formulated by, and in the interests of, those societal groups who have the power to translate their interests into law and policy.[168]

Power is a very important concept in Radical Criminology. Radical criminalists believe that the concept of power has two manifestations: one is the power of some groups to criminalize or decriminalize forms of behavior; the other is the power of some groups to evade being criminalized.[169] Two manifestations all reflect the greedy, egocentric, predatory, and exploitative nature of the powerful in capitalist society (usually capitalists, vested interests holders, and politicians serving capital), the hegemonic ideology, and the repression of people (working class, minority groups, powerless people).[170] The difference is:

The former shows that the powerful carry out a series of social constructions through their right to speak to realize their interests (moral or immoral, just or unjust, legal or illegal, charitable or exploitation) protection, for example, the protection of private property. This protection is generally achieved through criminal legislation and criminal justice. For example, almost any form of infringement of private property rights has been written into the penal codes of most countries globally, such as theft, robbery, fraud, etc., accompanied by relatively severe penalties.

The latter manifests the abuse of their right to speak by those in power. Mass media and criminal legislation misled the broad and large number of relatively lower-class members in capitalist society.[171] They restrained people's imagination and clear thinking through criminal legislation; simultaneously, through the mass media under their control, they excited

[168] RICHARD QUINNEY: *Bearing Witness to Crime and Social Justice*. Albany, State University of New York Press, 2000; JAMES BANKS: Radical Criminology and the Techno-Security-Capitalist Complex. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. pp. 103-119.

[169] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017. p. 421.

[170] See. DAVID O. FRIEDRICHS: Radical Criminology in the United States: An Interpretive Understanding. In: JAMES A. INCIARDI (ed): *Radical Criminology: The Coming Crises*. Beverly Hills, California, Sage, 1980. 35-60.

[171] BRIAN G. SELLERS AND BRUCE A. ARRIGO: Postmodern Criminology and Technocrime. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 150-163.

the harmfulness and catastrophic nature of the behaviors written in the criminal code.[172] While creating contradictions among the lower class members, it shifts people's attention to crimes committed by powerful people to relatively simple and violent street crimes.[173] As everyone knows, the social harm of crimes committed by people with power is often far greater than those committed by ordinary people without power.[174] To give a simple example, let us compare the manipulation of market prices, tax evasion, environmental pollution and street theft, robbery, and fraud in our imagination.

After a brief introduction to the core concept of radical criminology, power, the core goal of this theoretical paradigm becomes clear at a glance. Specific to the application of Radical Criminology to the study of cybercrime, the application of this theory can be as summarized, as James Banks stated, "Radical Criminology can […] contest state-defined concepts of cybercrime, oppose the growth of intrusive surveillance regimes and call into question the degree to which technology protects rather than encroaches on citizen's civil rights."[175]

3.3.2 A Brief Introduction to Feminist Criminology

To some extent, inequality is arguably the origin of all conflict. Radical Criminology arose when criminologists reflected on the inequalities that existed between powerful and powerless members of society. Feminist criminology emerged when some criminologists began to think about the inequality between males and females. It is generally believed that Feminist Criminology originated from the feminist movement in the 1960s and 1970s.[176]

---

[172] See. NICHOLAS GANE: The Governmentalities of Neoliberalism: Panopticism, Post-Panopticism and beyond. *The Sociological Review*, vol. 60. no. 4. (2012) 611-634; NANCY A. HEITZEG: Education or Incarceration: Zero Tolerance Policies and the School to Prison Pipeline. *Forum on Public Policy Online*, vol. 2009. no. 2. (2009) 1-21. [These two articles discuss the zero-tolerance policy and school management. Through legislation, combining the school's budget with the student's assessment results and introducing this capitalist market-based management model will lead the school to adopt a zero-tolerance policy. Based on the zero-tolerance policy, the school will monitor students in all directions. However, when schools and society enforce laws, they rarely reflect on whether this market-based approach is justified, especially in education. Legislation diverts people's attention, fixes people on the surface, and prevents people from thinking about the deep logic behind them. Media reports also played a role in fueling the flames.]

[173] BRIAN G. SELLERS AND BRUCE A. ARRIGO, 2018. p. 142.

[174] *See. e.g.*, EDWIN H. SUTHERLAND: Is "White Collar Crime" Crime? *American Sociological Review*, vol. 10. no. 2. (1945) 132-139; HAZELL CROALL: *Understanding White Collar Crime*. Buckingham, United Kingdom, Open University Press, 2001.

[175] JAMES BANKS, 2018. p. 119.

[176] MICHELE BURMAN AND LORAINE GELSTHORPE: Feminist Criminology: Inequalities, Powerlessness, and Justice. In: ALISON LIEBLING, SHADD MARUNA AND LESLEY MCARA (eds): *The Oxford Handbook of Criminology*. Oxford, Oxford University Press, 6th edition, 2017. pp. 213-238.

Carol Smart's book *Women, Crime, and Criminology: A Feminist Critique*, published in 1976, is an influential feminist criminology work. She points out that "criminology and sociology of deviance must become more than the study of men and crime if it is to play any significant part in the development of our understanding of crime, law, and the criminal process and play any role in the transformation of existing social practices."[177]

Traditional mainstream criminology historically overlooks gender and has been criticized by feminist criminologists as gender blindness.[178] Gender blindness can be stated as ignoring female criminals and victims; the general conclusions drawn from the study of male offenders apply to women without distinction. On the one hand, this can be understood as the inevitable outcome of a patriarchal society or androcentric culture. On the other hand, the significant proportion of men and boys among offenders has led traditional criminologists to focus more on men.[179] Feminist Criminology attempts to reverse gender blindness by theorizing the concept of gender. At the same time, Feminist Criminology questions the dichotomy of biological sex. The simple dichotomy of people in society regarding biological sex is narrow, inadequate, and stereotypical for the adequate study of gender and crime.

If we try to apply the theories of Feminist Criminology to understand crime and deviant behavior, we should not simply understand Feminist Criminology as a theoretical system whose research objects (including criminals and victims) are only females. Feminist criminology brings us more thoughts about the relationship between "gender" and "crime and criminal justice." This thinking can be further expanded to give greater attention to minorities and disadvantaged groups.[180] Feminist criminology, as a branch of Social Conflict Theory, inevitably includes the core concept of social conflict theory, power. Compared with men in social production and life dominated by patriarchy, women are powerless.[181] On the one hand, they are subject to the structural oppression of the patriarchal society, such as unfair education, political rights, and employment opportunities[182]; on the other hand, even in the

[177] CAROL SMART: *Women, Crime, and Criminology: A Feminist Critique*. London, Routledge, 1976.

[178] MEDA CHESNEY-LIND AND LISA PASKO: *The Female Offender: Girls, Women, and Crime*. Thousand Oaks, California, Sage, 2013.

[179] FRANCES HEIDENSOHN AND MARISA SILVESTRI: Gender and Crime. In: MIKE MAGUIRE, ROD MORGAN AND ROBERT REINER (eds): *The Oxford Handbook of Criminology*. Oxford, Oxford University Press, 2012. 5th edition, pp. 336-369.

[180] MICHELE BURMAN AND LORAINE GELSTHORPE, 2017. p. 222.

[181] ALISON J. MARGANSKI: Feminist Theory and Technocrime: Examining Gender Violence in Contemporary Society. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. pp. 11-34.

[182] JAMES W. MESSERSCHMIDT*: Capitalism, Patriarchy, and Crime: Toward a Socialist Feminist*

study of socially harmful behaviors---crimes and deviant behaviors---women are far less concerned than men, no matter as criminals or victims.

It is worth mentioning that in Feminist Criminology, "doing gender" is a very important paradigm to understand and explain crime. Women and men engage in doing gender in response to situated social hierarchies and expectations about masculinity and femininity, thus contributing to the reproduction of social structure.[183] Feminist Criminology treated crimes or deviant behaviors as resources of doing gender for men to achieve masculinity depending on men's or boys' social structural positions.[184] Obstacles to conventional success can lead to offending as a way to accomplish gender and show bravado. Machismo can be gained by exploiting others if no other avenues exist and in expressions of aggression and violence against devalued or oppressed groups. Then, violence against women, for example, translates as "proof" of one's masculinity; it shows that he is not frail to the person engaging in the behavior and others.[185]

3.3.3 Application of Radical/Feminist Criminology on Understanding Cybercrime

According to Larry J. Siegel's classification, Radical Criminology and Feminist Criminology fall within Social Conflict Theory. These two theories have received more academic attention and have produced rich empirical research results since modern times. As far as the study of cybercrime is concerned, the supporters of these two theories are more or less trying to understand and explain cybercrime within the framework of these two theories. The following part will briefly introduce two types of cybercrime, hacktivism and revenge pornography, based on the theoretical paradigm of Radical Criminology and Feminist Criminology.

The first is a discussion of criminal hacking. Since cybercrime has become an independent research theme, hacking has been a concern by relevant researchers. Originally, hackers referred to a group of technology enthusiasts with advanced computer and information technology[186], and hacking was seen as an innovative application of information

---

Criminology. Totowa, New Jersey, Roman and Littlefield, 1986.

[183] CANDACE WEST AND DON H. ZIMMERMAN: Doing Gender. *Gender & Society*, vol. 1. no. 2. (1987) 125-151.

[184] JAMES W. MESSERSCHMIDT: *Masculinities and Crime: Critique and Reconceptualization of Theory*. Lanham, Maryland, Rowman & Littlefield, 1993.

[185] ALISON J. MARGANSKI, 2018. p. 14.

[186] WESLEY CHAI: *What is a hacker?* TechTarget, 28 October 2021, https://www.techtarget.com/searchsecurity/definition/hacker

technology.[187] However, with the popularization of the civil and commercial Internet, some hackers use their technical advantages to invade specific computer information systems, interfere with the normal operation of the cyber system, and steal users' personal information and other behaviors to achieve a profit with improper purposes.[188] The technology itself is neutral, but the misuse of technology for illegitimate gains has become one of the fundamental reasons for the criminalization of hacking. Cracking down on hacker crime has become a universal consensus all over the world. If we stop there, there seems to be no need to rethink the criminalization of hacking through radical criminology. However, one of the landmarks that have prompted radical criminologists to reflect on the indiscriminate criminalization of hacking is the two-way interaction between information technology and democracy. [189] The wide popularization of information technology has broadened the channels for social members to participate in political life.[190] People can realize political participation and democracy by posting their comments, expressing their opinions, participating in voting, and supervising on the Internet.[191] However, social members' political participation forms are not always gentle and acceptable to the class at the power center. When some members express relatively radical views on the Internet, people with power will take certain measures to limit their online political participation to maintain their vested interests; for example, hacktivism will be criminalized.

Unlike general hacking, hacktivism is a new form of protest that follows democratic principles and defends and safeguards human rights.[192] Hacktivists challenge social injustices caused by states, corporations, and other power centers by employing a range of technological activities, such as distributed denial-of-service attacks, website defacement, virtual sit-ins, and information theft.[193] To some extent, these actions have encroached on the

[187] MAJID YAR AND KEVIN F. STEINMETZ: *Cybercrime and Society*. London, Sage, 2019. 3rd edition. pp. 53-54.

[188] MAJID YAR AND KEVIN F. STEINMETZ, 2019. p. 158

[189] JAMES BANKS, 2018. p. 106.

[190] See. MANUEL CASTELLS: The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. *The ANNALS of the American Academy of Political and Social Science*, vol. 616. no. 1. (2008) 78-93.

[191] See. e.g., ZHENGLIANG CHEN AND RONG ZHOU: On the Role and Perfection of Citizen Online Political Participation in Democratic Political Construction [论公民网络政治参与在民主政治建设中的作用及其完善]. *Academic Journal of Zhongzhou* [中州学刊], no. 1. (2011) 17-20.

[192] NOAH C.N. HAMPSON: Hacktivism: A New Breed of Protest in A Networked World. *Boston College International and Comparative Law Review*, vol. 35. no. 2. (2012) 511-542.

[193] PAUL A. TAYLOR: From Hackers to Hacktivists: Speed Bumps on the Global Superhighway? *New Media & Society*, vol. 7. no. 5. (2005) 625-646.

interests of the class at the power center. Therefore, the class of the power center represented by the state brings these behaviors into general hacking without distinction and criminalizes it. Radical criminologists believe that the criminalization of hacktivism is a violation of the political participation and democratic rights of the powerless by the powerful in a capitalist society. This kind of infringement usually falls into three steps: first is blurring the boundary between criminal hacking and hacktivism[194]; in other words, criminal hacking and hacktivism are conflated through the definition of general criminal legislation. Secondly, through the mass media controlled by the powerful, the powerful classes render social members perception of the danger and urgency of cybercrime, create security anxiety, and distract people's attention [from the unjust behavior of the powerful class to the illusionary possibility of becoming victims].[195] Third, based on the former two approaches, people should be encouraged to pursue information security. In order to alleviate security anxiety and pursue information security, people have to accept stricter supervision and control from the state and corporates;[196] meanwhile, some companies offering Internet security products took advantage of this to peddle their products and expand the market.[197] It restricts citizens' basic human rights and obtains improper interests, which embodies the greed, cunning, and selfishness of the powerful class in the capitalist society everywhere.

Then there is the discussion of the crime of revenge pornography. The crime of revenge pornography usually occurs in an intimate relationship. It is the behavior of the offender to share the victim's private photos, videos, and other forms of multimedia files with sexual innuendo and sexual description with a third party without the victim's consent.[198] Usually, when criminals upload or share these multimedia files, they also attach the victim's

[194] See. TIM JORDAN AND PAUL A. TAYLOR: *Hacktivism and Cyberwars: Rebels with a Cause?* London, Routledge, 2004.

[195] See. DAVID S. WALL: Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers & Technology*, vol. 22. no. 1-2. (2008) 45-63; JAMES BANKS, 2018. p. 110.

[196] See. MAJID YAR AND KEVIN F. STEINMETZ, 2019. 73-77; TIM JORDAN: Language and Libertarianism: The Politics of Cyberculture and the Culture of Cyberpolitics. *The Sociological Review*, vol. 49. no. 1. (2001) 1-17; JAMES BANKS, 2018. 109-112.

[197] See. JAMES BANKS: The Heartbleed Bug: Insecurity Repackaged, Rebranded and Resold. *Crime, Media, Culture*, vol. 11. no. 3. (2015) 259-279; MAJID YAR: Computer Crime Control as Industry: Virtual Insecurity and the Market for Private Policing. In: KATJA FRANKO AAS, HELENE OPPEN GUNDHUS AND HEIDI MORK LOMELL (eds): *Technologies of Insecurity: The Surveillance of Everyday Life*. London, Routledge-Cavendish, 2008. 189-204.

[198] DANIELLE K. CITRON AND MARY A. FRANKS: Criminalizing Revenge Porn. *Wake Forest Law Review*, vol. 49. no. 2. (2014) 345-391.

name, address, telephone number, and other personal information.[199]

On the one hand, because of the fast spread of the Internet, when private information associated with sexual description files is uploaded to cyberspace, the harm it causes exceeds the traditional way of sharing, usually characterized by illegal profit and destroys the victim's reputation.[200] On the other hand, due to the anonymity of the Internet, such criminals can often use technology to hide their IP addresses to avoid the risk of a criminal investigation. In general, it is difficult or costly to identify the real IP address of a specific criminal based on existing technology.[201] Therefore, it can be said that the Internet has been applied to facilitate, perpetrate and communicate such crimes.[202]

Due to the characteristics of low "cost," high "profits," great harm, and difficult investigation, increasing criminal legislation and academic research gradually began to respond to the crime of revenge pornography. Feminist Criminology plays a significant role in understanding and explaining the crime of revenge pornography.[203]

Feminist criminology believes that the crime of revenge pornography is the byproduct of hegemonic masculinity in a patriarchal society, which is manifested as the exploitation of powerless and vulnerable groups (usually women) by powerful people (usually men).[204] According to the different motives, the crime of revenge pornography can be divided into the illegal profit-making type and reputation-destroying type.

The illegal profit-making type is represented by the unauthorized uploading and selling of multimedia files containing the victims' sexual activities for-profit and the extortion of the victims.[205] Specifically, uploading the files to the Internet is a threat, and the victims are coerced to pay or meet criminals' other needs. It reflects that in the androcentric society, male members naturally overlook or underestimate the identity of female members (or sexual minorities) and instrumentalize and objectify victims rather than treat victims as

[199] DANIELLE KEATS CITRON: Law's Expressive Value in Combating Cyber Gender Harassment. *Michigan Law Review*, vol. 108. no. 3. (2009) 373–415.

[200] KATLYN M. BRADY: Revenge in Modern Times: The Necessity of a Federal Law Criminalizing Revenge Porn. *Hastings Women's Law Journal*, vol. 28. no. 1. (2017) 3-24.

[201] See. e.g., DAWEI SONG: The Criminal Governance of 'QR Code' Crime [二维码犯罪的刑事治理]. *Journal of Heilongjiang Administrative Cadre College of Politics and Law* [黑龙江省政法管理干部学院学报], no. 5. (2017) 32-35.

[202] ALISON J. MARGANSKI, 2018. p. 20.

[203] ALISON J. MARGANSKI, 2018. p. 17.

[204]AMANDA BURGESS-PROCTOR: Intersections of Race, Class, Gender, and Crime: Future Directions for Feminist Criminology. *Feminist Criminology*, vol. 1. no. 1. (2006) 27-47.

[205] ALISON J. MARGANSKI, 2018. p. 20.

subjects equal to themselves.[206]

The reputation-destroying type shows that the main purpose of revenge pornography is to destroy the victim's reputation. After a heterosexual relationship ends, men often assume that the woman's infidelity caused the relationship to end. The male may perceive his own experience of frustration, repression, and pain as a sign of failure. This failure is the male's failure to realize his masculinity or the failure of gender practice. Insofar as compensating for this frustration, the male falsely reclaims his masculinity by uploading revenge pornography accompanied by personal information about the victim.[207] After a homosexual relationship ends, the person who suffered frustration will retaliate in the same way above. If it is a lesbian relationship, the possibility of the perpetrator destroying the victim's reputation to achieve revenge lies in the inherent prejudice or stereotypes against women or girls in doing differences in the patriarchal society. If it is a gay relationship, the feasibility of the perpetrator's revenge lies in the victim's failure to fulfill the gendered expectations of men or boys in the patriarchal culture.[208]

To sum up, we can find that the bidirectional oppression of males and females by hegemonic masculinity in a patriarchal society criticized by Feminist Criminology is the cause and underlying logic of the harm of revenge pornography. Under the dominance of hegemonic masculinity, men (the powerful) are not necessarily the beneficiaries. Conversely, men (especially in sexual minorities) and women (the powerless) constitute oppressed groups.[209] Furthermore, revenge pornography could arguably not bring about such harm to victims compared with the situation nowadays, and eliminated victims' panic and anxiety coping with revenge porn from the root only if in a society whose male members and female ones were equal and would not be labeled or stigmatized for the failure of doing gender.

3.3.4 Comments

The above application of Radical Criminology and Feminist Criminology in explaining and understanding cybercrime shows that it is feasible to understand and explain

---

[206] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017. pp. 288-295.

[207] See. MATTHEW HALL AND JEFF HEARN: Revenge Pornography and Manhood Acts: A Discourse Analysis of Perpetrators' Accounts. *Journal of Gender Studies*, vol. 28. no. 2. (2019) 158-170.

[208] See. R. W. CONNELL AND JAMES W. MESSERSCHMIDT: Hegemonic Masculinity: Rethinking the Concept. *Gender & Society*, vol. 19. no. 6. (2005) 829-859; FRANCES HEIDENSOHN AND MARISA SILVESTRI, 2012. p. 348.

[209] ALISON J. MARGANSKI, 2018. p. 16.

cybercrime through social conflict theory. Unlike social structure theory and social process theory, social conflict theory is at a relatively macroscopic theoretical level and provides a series of heuristic reflections and innovative structures for cybercrime researchers. In terms of understanding and explaining cybercrime, the research paradigm of Radical Criminology does not stick to the micro-structure of a particular crime and its interaction but broadens its vision to the contradictions and conflicts among various social classes. Its practical significance lies in analyzing the inherent contradictions of each class in a capitalist society, questioning and reflecting on the practice of Internet crime legislation, law enforcement, and judicial practice, and encouraging a prudent, balanced, and convergent attitude towards the criminalization of Internet deviant behavior. Based on gender inequality in a capitalist society, Feminist Criminology has experienced a process from discussing gender difference, combining the basic view of social conflict, and then to the fairness of minority groups in society. This process shows that although Feminist Criminology is named "feminism," it has gradually been extended to the criminology theory concerned with minority groups.[210] The expansion of this theoretical field marks the maturity of Feminist Criminology and its capability to explain the generality of various types of crime.

However, Radical Criminology and Feminist Criminology also have certain limitations in understanding and explaining cybercrime.

The gene of criticizing everything and questioning everything in Radical Criminology makes it inevitable that the research on cybercrime within Radical Criminology has prominent political characteristics. The logical premise of Radical Criminology is the conflict of power. In the research, how to operationalize and measure the power conflict directly affects the conclusion's validity. Take hacktivism as an example. Theoretically, researchers can distinguish hacktivism from hacking by conceptual design. However, what criteria do researchers use to judge whether an act is hacking or hacktivism in practice? Objectively, there are overlaps between hacking and hacktivism. Therefore, the main criterion to distinguish hacking from hacktivism is the conclusion of contextual analysis based on the subjective aspect of the crime committed by the parties and their social background. It is inevitably subjective the study of Radical Criminology. The consequence of subjectivist research is that it is difficult to distinguish between the results of a specific researcher and those of Radical Criminology.

[210] MICHELE BURMAN AND LORAINE GELSTHORPE, 2017. p. 222.

The shift of Feminist Criminology towards the justice of minority groups is laudable. However, the inherent shortcomings of Feminist Criminology will lead to the regression of this theory in the process of guiding judicial practice and social reform. Specifically, while the social allocation pays attention to minority groups, the conclusions drawn by the study of majority groups are, according to feminist criminology, hardly compatible with the real interests of minority groups. On the one hand, when minority groups receive certain attention, corresponding policies and legislation will also consider the unique needs of minority groups and make adjustments accordingly. Nevertheless, as it turns out, these adjustments do not necessarily produce the results those female criminologists expect; these unintended consequences can backfire.[211] On the other hand, when we assumed that policy and legislative adjustments have the desired effect, the problem of *Reverse Discrimination* by general groups against specific groups emerged[212]

3.4 STAGED SUMMARY

As stated at the beginning of this part, the criminological theory research on the causes of cybercrime is insufficient. This part starts from the relevant theories of sociological approaches in criminology, through their categorization by Larry J. Siegel, briefly reviews the basic views of Merton's Strain Theory and Agnew's General Strain Theory in Social Structure Theory, Sutherland's Differential Association Theory, and Burgess' Criminological Social Learning theory in Social Process, and Radical Criminology and Feminist Criminology in Social Conflict Theory; and evaluates those applications to cybercrime research. The fundamental assumption of the sociological approaches in criminology acknowledges the impact of technological progress on crime, so this part chooses the sociological approaches in criminology to understand and explain cybercrimes. It is worth noting that when this part discusses the application of the sociological approaches in criminology to cybercrime, it expresses the mode of "understanding" and "explanation." They show that this part is launched around the etiology of cybercrime. The purpose of

[211] See. e.g., JENNIFER TEMKIN AND BARBARA KRAHÉ: *Sexual Assault and the Justice Gap: A Question of Attitude*. Oxford, Hart Publishing, 2008. pp. 9-28; MICHELE BURMAN: Evidencing Sexual Assault: Women in the Witness Box. *Probation Journal*, vol. 56. no. 4. (2009) 379-398; NICOLE WESTMARLAND: Still Little Justice for Rape Victim Survivors: The Void between Policy and Practice in England and Wales. In: NICOLE WESTMARLAND AND GEETANJALI GANGOLI (eds): *International Approaches to Rape*. Bristol, The Policy Press, 2011. pp. 79-100.

[212] FINDLAW'S TEAM OF LEGAL WRITERS AND EDITORS: *Reverse Discrimination*. FindLaw, 28 October 2021, https://www.findlaw.com/employment/employment-discrimination/reverse-discrimination.html [It will not expand here, for details, see *Regents of the University of California v. Bakke*, 438 U.S. 265 (1978)].

utilizing different theories within social approaches in criminology to understand and explain the etiology of different cybercrimes is to generate a pluralistic, integrated, and developing paradigm for conceiving the impact of technical evolution, as a kind of social construction, on cybercrime and considering the reason of distinct behavioral performances of cybercriminals. Through the previous introduction of this part, it is not difficult to find that the causes leading to cybercrimes are not all attributable to individual choices. *The human being must be understood as a social person.*[213] Because of this, the anomie of the overall cultural goals of the society, differential associations and unacceptable learnings produced by situated environments of individuals, the power conflict rooted in social construction and gender inequality all "induce" or "force" a certain number of social members to engage in cybercrimes to a certain extent. Then, when we reflect on responses to crime, if we solely rely on the conviction and sentencing of criminal code provisions to punish perpetrators rather than apply social policies, which are arguably potent but out of the scope of criminal law, to cope with cybercrime, it will presumably create a split among social members and society.

[213] See. JOEL M. CHARON: *Symbolic Interactionism: An Introduction, An Interpretation, An Integration*. United States, Pearson, 2010. 10th Edition.

III. LEGAL MEANS AGAINST CYBERCRIME IN CHINA: THE LEGISLATIVE PRACTICE

Policies, Legislations, & Regional International Cooperation in China

1. A GLANCE AT CHINESE LEGAL SYSTEM

This chapter examines China's legislative framework for regulating cyberspace and combating cybercrime. This chapter will discuss China's legal framework for coping with cybercrime on both the international and domestic levels. At the international level, analysis of China's regional international cooperation is primarily conducted through the Shanghai Cooperation Organization. The domestic level will introduce China's cyberspace governance policies, cyber laws and regulations, and cybercriminal laws to deal with cybercrime. Before proceeding to the following sections, this section will briefly describe the basic characteristics of China's legal system and the source of current Chinese law.

1.1 SOCIALIST LEGAL SYSTEM WITH CHINESE CHARACTERISTICS

There are three main legal genealogies in the current world: the common law system, the civil law system, and the socialist law system represented by the laws of the former Soviet Union and Eastern European countries.[214] China does not fall into any of the three categories. China's legal system is summarized as a socialist legal system with Chinese characteristics [中国特色社会主义法律体系].[215] China's national circumstances are unique. China's mainland adheres to a socialist political system. Hong Kong, Macau, and Taiwan all adhere to capitalism. In terms of legal systems, mainland China is socialist, Hong Kong is common law, Macao is civil law, and Taiwan has its own peculiarities.[216] As a result, it is

[214] See. RENÉ DAVID AND JOHN E. C. BRIERLEY: *Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law*. New York, The Free Press, 1978.

[215] In 1997, the 15th National Congress of the Communist Party of China set the goal of forming a socialist legal system with Chinese characteristics by 2010. This objective was pursued as a political task until 2010. Wu Bangguo, the chairman of the Standing Committee of the National People's Congress, announced at the Fourth Session of the Tenth National People's Congress in 2010 that a socialist legal system with Chinese characteristics had taken shape. See. *Jiang Zemin's Report at the 15th National Congress of the Communist Party of China* [江泽民在中国共产党第十五次全国代表大会上的报告], 12371.cn, 20 March 2022, https://fuwu.12371.cn/2012/09/27/ARTI1348726215537612_all.shtml; *Wu Bangguo's Speech at the Fourth Session of the Eleventh National People's Congress* [吴邦国在第十一届全国人民代表大会第四次会议上的讲话], The National People's Congress of The People's Republic of China, 20 March 2022, http://www.npc.gov.cn/zgrdw/npc/dbdhhy/11_4/2011-07/06/content_1871271.htm

[216] WENXIAN ZHANG: *Jurisprudence* [法理学]. Beijing, Peking University Press & Higher Education Press,

difficult to classify China as common law, civil law, or socialist law system.

However, as far as mainland China is concerned, its legal system has the following characteristics:

First, in terms of the source of law, mainland China's formal source of law is statutory law; court precedents, legal scholarships, etc., have no legal effect.

Second, in terms of codification, mainland China enacts laws in the form of codes, such as the Criminal Law of the People's Republic of China [中华人民共和国刑法] and the Civil Code of the People's Republic of China [中华人民共和国民法典].

Third, in terms of the application of legal techniques, when hearing a case, the judges of mainland China first consider the provisions of the statutory law in addition to the facts of the case and then adjudicate the case in accordance with the relevant provisions.

Fourth, China's judicial system is distinct from the inquisitorial litigation model prevalent in civil law countries and the adversarial litigation model prevalent in common law countries.[217] It is especially pronounced in China's criminal justice system. In 2016, mainland China initiated a trial-centered reform of the criminal procedure system.[218] As far as criminal proceedings are concerned, China's criminal justice system is "trial-centered [以审判为中心]." Trial-centeredness here should be understood as centered on substantive trial activities. This is consistent with China's institutional framework for criminal proceedings.[219] In China, criminal proceedings have three stages: investigation, prosecution, and trial. Usually, the public security organ is responsible for investigation; prosecution is the responsibility of the

---

2011. 4th edition, p. 158.

[217] Some scholars argued that Chinese legal system is an inquisitorial system. (See. WEIMEI PAN AND LUCIANA DURANTI: Sitting in Limbo or Being the Flaming Phoenix: The Relevance of the Archival Discipline to the Admissibility of Digital Evidence in China. *Archives and Manuscripts*, vol. 48. no. 3. (2020) 300-327. ["As opposed to the adversarial system adopted in common law system, the Chinese legal system is an inquisitorial system, the prevailing system in civil law jurisdictions, including continental Europe and Latin America."]) However, by the legal reform, this kind of recognition should be changed from this dissertation's viewpoint. Chinese judicial system is a mixed one to some extent and has its own specialties.

[218] See. *Notice of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Issuing the Opinions on Advancing the Reform of the Trial-Centered Criminal Procedure System* [最高人民法院、最高人民检察院、公安部、国家安全部、司法部印发《关于推进以审判为中心的刑事诉讼制度改革的意见》的通知], Supreme People's Procuratorate of the People's Republic of China, 11 October 2016, https://www.spp.gov.cn/zdgz/201610/t20161011_169052.shtml

[219] YONGZHONG GU: *The Meaning of "Trial-Centered" as It Should Be* ["以审判为中心"的应然涵义], Procuratorial Daily [检察日报], 11 December 2019, http://newspaper.jcrb.com/2019/20191211/20191211_003/20191211_003_3.htm

procuratorate; the trial is the responsibility of the court.[220] These three stages have different divisions of labor, cooperate with each other, and check each other.[221] In China, criminal trials are a collaborative effort between the prosecution (procuratorate), the defense (defendant and his lawyer), and the trial (judge). In court proceedings, the procuracy prosecutes the accused on behalf of the State; the defendant and his lawyer defend the crimes alleged by the procuratorate, and the judge presides over the trial proceedings and may also exercise his or her authority to interrogate the accused.[222] As a result, China's litigation model incorporates both inquisitorial and adversarial elements.

Fifth, in terms of legal classification, mainland China does not simply divide the law into public and private law, or common law and equity. The legal system of mainland China has been summarized as follows: a socialist legal system with Chinese characteristics based on China's national conditions and reality, adapting to the needs of reform, opening up, and socialist modernization, and embodying the will of the party and the people in a concentrated way, with the Constitution as the commander-in-chief, with the laws of seven legal departments, including the constitution-related law, civil and commercial law, administrative law, economic law, social law, criminal law, litigation and non-procedural law, as the backbone, and the legal norms at three levels, including laws, administrative regulations, and local regulations.[223]

1.2 SOURCE OF LAW IN MAINLAND CHINA TODAY

The term "Source of Law" refers to a variety of things: (1) agents (individual officials or institutions) authorized to make law; (2) the products of such agents' lawmaking activities; (3) interpretive materials bearing on the content of legal norms; and (4) the legal validity criteria that operate in a legal system.[224] In light of this classification, this section will

[220] See. *Criminal Procedure Law of the People's Republic of China* [中华人民共和国刑事诉讼法]: Part II-Opening a Case, Criminal Investigation and Initiation of Public Prosecution［第二编-立案、侦查和提起公诉］; and Part III-Trial [第三编-审判].

[221] See. Article 140 of *Constitution of the People's Republic of China* [中华人民共和国宪法]: The people's courts, the people's procuratorates and the public security organs shall, in handling criminal cases, divide their functions, each taking responsibility for its own work, and they shall coordinate their efforts and check each other to ensure the correct and effective enforcement of the law [人民法院、人民检察院和公安机关办理刑事案件，应当分工负责，互相配合，互相制约，以保证准确有效地执行法律].

[222] See. Article 191 of *Criminal Procedure Law of the People's Republic of China* [中华人民共和国刑事诉讼法]: A judge may question a defendant [审判人员可以讯问被告人].

[223] See. JINGWEN ZHU: The Socialist Legal System with Chinese Characteristics: Its Structure, Features and Trends. *Social Sciences in China*, vol. 32. no. 3. (2011) 87-103.

[224] FÁBIO P. SHECAIRA: *Legal Scholarship as a Source of Law*. New York, Springer, 2013, p. 9.

examine which organs have legislative authority in China's political context and the types of normative documents these organs formulated through legislative authority. See Figure III. 1.2-1

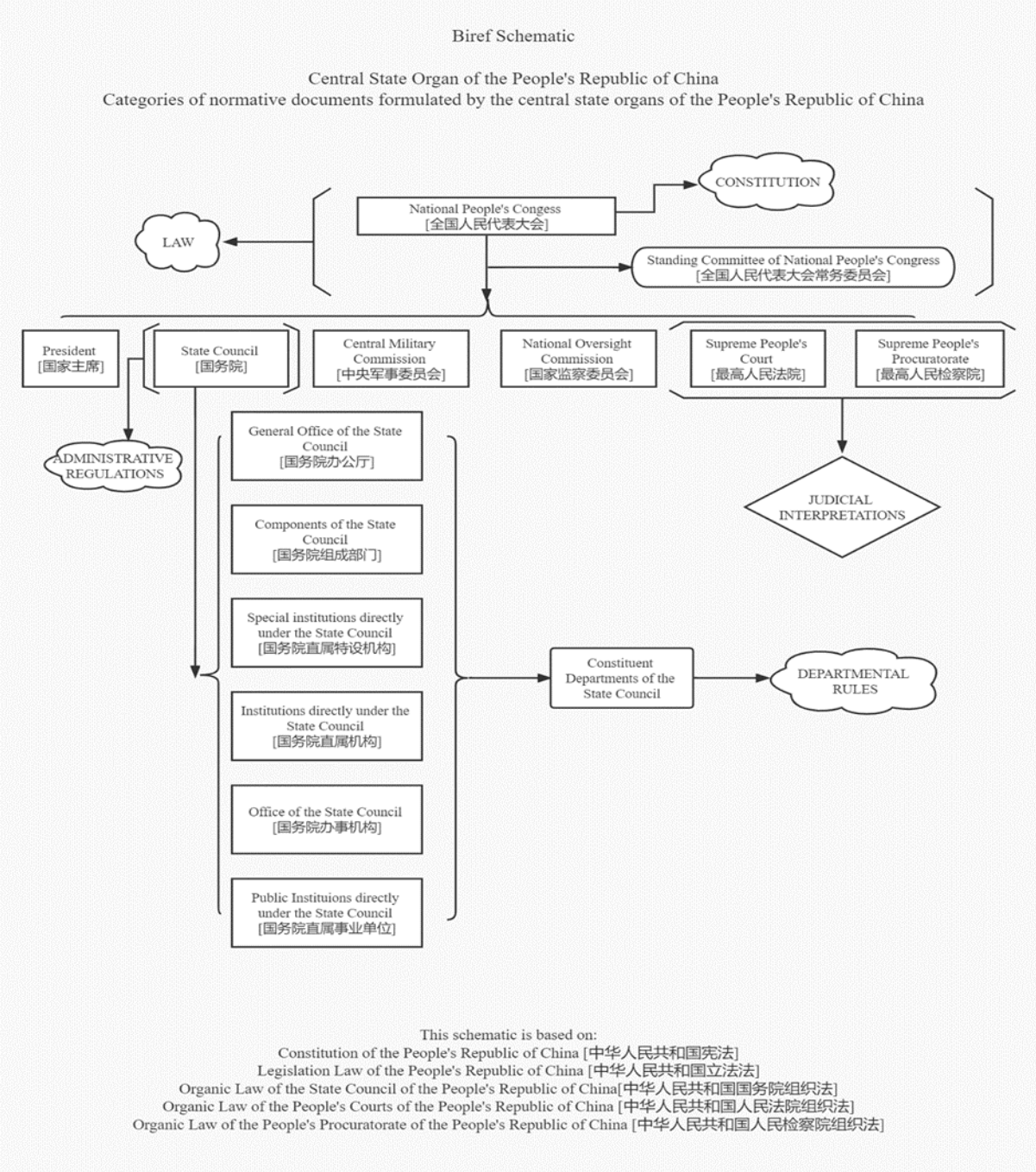

Figure III. 1.2-1 Brief schematic of State Power and Normative Documents' type in mainland China at the national central level

1.2.1 Structure of State Power in China: National Central Level[225]

[225] Not all of China's central state organs have been expanded, and this subsection deals only with state institutions related to subsequent subsections of this chapter.

The highest organ of state power in China is the National People's Congress of the People's Republic of China. The National People's Congress shall set up a Standing Committee as a permanent body to exercise some of the functions of the National People's Congress in accordance with the Constitution when the National People's Congress is not in session.[226] The National People's Congress and Standing Committee thereof exercise state legislative power.[227]

The President of the People's Republic of China, the State Council, the Central Military Commission, the Supreme People's Procuratorate, the Supreme People's Court and the National Oversight Commission are produced by the National People's Congress.[228] Among them, the State Council (Central People's Government) is the highest administrative organ in China. The State Council is composed of the Premier, Vice Premiers, State Councilors, Ministers, Committee Chairmen, Auditor-General and Secretary-General.[229] The organizational structure of the State Council includes[230]: the General Office of the State Council, the Components of the State Council[231], the Special Institutions directly under the State Council, the Institutions directly under the State Council, the Offices of the State Council, the Public Institutions directly under the State Council, and the State Bureau managed by the ministries and commissions under the State Council.[232] The Supreme People's Procuratorate is the highest legal supervisory organ in China.[233] The Supreme People's Court is the highest judicial organ in China.[234]

1.2.2 Formal Source of Law in mainland China

The formal source of law in contemporary China is manifested in the form of various statutory laws with the Constitution as the core. The specific performance is as follows:

---

[226] See. Article 57 of *Constitution of the People's Republic of China* [中华人民共和国宪法]

[227] See. Article 58 of *Constitution of the People's Republic of China* [中华人民共和国宪法]

[228] See. Chapter III-The Structure of the State [第三章-国家机构] in *Constitution of the People's Republic of China* [中华人民共和国宪法]

[229] See. Article 85 & Article 86 of *Constitution of the People's Republic of China* [中华人民共和国宪法]

[230] See. *Notice of the State Council on the Setup of Institutions (2018), No. 6 [2018] of the State Council* [国务院关于机构设置的通知 (2018)，国发〔2018〕6号]

[231] In current mainland China (2018 to now), the Components of the State Council include twenty-one ministries, three commissions, People's Bank of China [中央人民银行], and National Audit Office [审计署].

[232] There are thirteen state bureaus managed by the ministries and commissions under the State Council. Because they are managed by the components of the state council, they do not appear in Figure III. 1.2-1 as an independent branch of constituent departments of the State Council.

[233] See. Article 137 of *Constitution of the People's Republic of China* [中华人民共和国宪法]

[234] See. Article 132 of *Constitution of the People's Republic of China* [中华人民共和国宪法]

Constitution [宪法]. China's Constitution is established in the form of statutory law. The Constitution is the fundamental law of China and the main source of China's socialist laws. The Constitution has the highest legal validity, and no laws, administrative regulations or local regulations shall conflict with the content of the Constitution. Only the National People's Congress in China has the authority to amend the Constitution. The Standing Committee of the National People's Congress has the authority to interpret the Constitution and supervise its enforcement.[235]

Laws [法律][236]. In China, the law is second only to the Constitution in importance. China's laws can be classified into two categories based on their enactment organs: basic laws enacted and revised by the National People's Congress, which include criminal, civil, state organs, and other fundamental laws[237]; and non-basic laws enacted by the Standing Committee of the National People's Congress.[238] When the National People's Congress is not in session, the Standing Committee has the authority to amend and supplement basic laws, but they must not contradict those laws' fundamental principles.[239] Simultaneously, resolutions or decisions of the National People's Congress and its Standing Committee are considered laws if they contain a normative provision rather than a document such as a general declaration or an appointment order.[240]

Administrative regulations [行政法规]. Administrative regulations are normative documents governing state administrative management activities that are drafted by the State's highest administrative organ (the State Council) in accordance with the Constitution and laws and in order to carry them out. Administrative regulations constitute a significant body of source of law in China. Administrative regulations rank third in validity behind the Constitution and laws. Simultaneously, normative decisions or orders issued by the State Council are also formal sources of law.[241]

---

[235] See. Article 62 & Article 67 of *Constitution of the People's Republic of China* [中华人民共和国宪法]

[236] Laws here refer only to normative documents formulated by the National People's Congress and its Standing Committee.

[237] See. Article 62 of *Constitution of the People's Republic of China* [中华人民共和国宪法] & Article 7 of Legislation Law of the People's Republic of China [中华人民共和国立法法]

[238] See. Article 67 of *Constitution of the People's Republic of China* [中华人民共和国宪法] & Article 7 of Legislation Law of the People's Republic of China [中华人民共和国立法法]

[239] Ibid.

[240] GUOYING SHU: *Introduction to Jurisprudence* [法理学导论]. Beijing, Peking University Press, 2019. 3rd edition, p. 73.

[241] Ibid.

Departmental rules [部门规章]. Departmental rules refer to all kinds of normative legal documents of an administrative nature formulated by constituent departments with administrative management functions under the State Council[242] in accordance with laws and administrative regulations, decisions and orders of the State Council, and within the scope of their administrative authority.[243] Departmental rules have a lower status than the Constitution, laws and administrative regulations and must not contradict them.

1.2.3 Informal Source of Law in mainland China

Customs. Current Chinese law is primarily based on statutory law, but some customs may be recognized in exceptional circumstances. For example, the Civil Code of the People's Republic of China states that when dealing with civil disputes, if no relevant legal provision exists, customs may be applied. They must not, however, violate public order or good morals.[244] Furthermore, the Law of the People's Republic of China on Regional National Autonomy states that all ethnic minorities in ethnic autonomous areas have the freedom to preserve and reform their own customs and folkways.[245] The term "customs" here primarily

[242] Not all constituent departments of the State Council have administrative functions, for example, the Offices of the State Council. The Offices of the State Council do not have independent administrative functions, according to Article 6 of the Regulations on Administration of the Establishment and Staffing of the Administrative Agencies of the State Council. As a result, according to Article 80 of the Legislation Law of the People's Republic of China, the Offices of the State Council lack the authority to enact departmental rules. It is worth mentioning that the Cyberspace Administration of China (CAC), which is mainly involved in this dissertation, is one of the Offices of the State Council. Under the aforementioned law, it did not have the authority to make departmental regulations at the time of its establishment (May 2011). It was not until August 2014 that the State Council authorized the reorganized CAC to be in charge of managing information on the Internet on a national scale, as well as supervising and administering law enforcement. CAC now has administrative management authority and is qualified to enact departmental rules. See. Article 6 of the *Regulations on Administration of the Establishment and Staffing of the Administrative Agencies of the State Council* [国务院行政机构设置和编制管理条例]: The Offices of the State Council assist the Premier of the State Council in handling specialized affairs and do not have independent administrative functions [国务院办事机构协助国务院总理办理专门事项，不具有独立的行政管理职能]; Article 80 of the *Legislation Law of the People's Republic of China* [中华人民共和国立法法]: The ministries and commissions of the State Council, the People's Bank of China, the National Audit Office, and other institutions with administrative functions directly under the State Council may, in accordance with the laws and the administrative regulations, decisions, and orders of the State Council, enact departmental rules within their respective power [国务院各部、委员会、中国人民银行、审计署和具有行政管理职能的直属机构，可以根据法律和国务院的行政法规、决定、命令，在本部门的权限范围内，制定规章]; *Notice of the State Council on Charging the Cyberspace Administration of China with the Content Management of Information on the Internet, No. 33 [2014] of the State Council* [国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知，国发〔2014〕33 号].

[243] See. Article 80 of the *Legislation Law of the People's Republic of China* [中华人民共和国立法法]

[244] See. Article 10 of the *Civil Code of the People's Republic of China* [中华人民共和国民法典]

[245] See. Article 10 of the *Law of the People's Republic of China on Regional National Autonomy* [中华人民共

refers to ethnologic customs. As a result, ethnologic customs can be considered a type of source of Chinese law, though not all ethnologic customs are the source of law.

Precedents. In China, precedents do not have the status of a formal source of law. China's judicial practice, however, does not deny the role of typical cases as a reference. Guiding Cases may be issued in China by the Supreme People's Court and the Supreme People's Procuratorate.[246] Guiding Cases shall be referred to by people's courts or procuratorates when dealing with similar cases.[247] The reference to Guiding Cases, on the other hand, can only be reflected in the legal reasoning. Guiding Cases cannot be used to replace the law, that is, as the basis for adjudication in a judgment or as a legal basis in an indictment.[248]

Policies. The academics of Chinese jurisprudence scholarship generally hold that in China, policies are generally divided into state policies and the policies of the Communist Party of China. Some of the state policies and the policies of the Communist Party of China (CPC) have been embodied in the Constitution and various enacted laws. These policies are, of course, the formal source of law. Policies that are not reflected in the enactment of laws, especially those of the CPC, are informal sources of law. This is because the CPC is the ruling party, and its leadership over China as the ruling party is mainly achieved by formulating correct policies. Therefore, the policies of the CPC play a direct guiding role in the formulation and implementation of Chinese law.[249] Some non-Chinese scholars argue that the Chinese government's approach to law is fundamentally instrumentalist. It means that laws and regulations are intended to be instruments of policy enforcement, and are explicitly to achieve the immediate policy objectives of the regime.[250] Meanwhile, Pitman B. Potter,

---

和国民族区域自治法]

[246] See. Article 18 of the *Organic Law of the People's Courts of the People's Republic of China* [中华人民共和国人民法院组织法] & Article 23 of the *Organic Law of the People's Procuratorates of the People' Republic of China* [中华人民共和国人民检察院组织法].

[247] See. Article 7 of the *Provisions of the Supreme People's Court on Case Guidance* [最高人民法院关于案例指导工作的规定] & Article 15 of the *Provisions of the Supreme People's Procuratorate on Case Guidance* [最高人民检察院关于案例指导工作的规定]

[248] See. Article 10 of the *Detailed Rules for the Implementation of the Provisions of the Supreme People's Court on Case Guidance* [《最高人民法院关于案例指导工作的规定》实施细则] & Article 15 of the *Provisions of the Supreme People's Procuratorate on Case Guidance* [最高人民检察院关于案例指导工作的规定]

[249] See. WENXIAN ZHANG, 2011, p. 58; GUOYING SHU, 2019, pp. 84-85.

[250] See. XINGZHONG YU: Legal Pragmatism in the People's Republic of China. *Journal of Chinese Law*, vol. 3. no. 1. (1989) 29-52; RONALD C. KEITH: *China's Struggle for the Rule of Law*. London, Palgrave Macmillan UK, 1994, pp. 218-221.

after a thorough analysis of China's legal institutions, found that the development of Chinese legal institutions and practices has reflected particularly the imperatives of political control for the CPC.[251]

1.3 A Brief Discussion of China's Judicial Interpretations

In China, official interpretations of laws are classified into two categories: legal (or legislative) interpretations and judicial interpretations.

The Standing Committee of the National People's Congress has the authority to interpret laws. Legal interpretation is the interpretation of laws made by the Standing Committee. According to Chinese scholars, its validity is equivalent to that of laws.[252] Judicial interpretations fall into two categories. Trial interpretation is the Supreme People's Court's interpretation of the law as it pertains to the specific application of the law during trial proceedings. Procuratorial interpretation refers to the Supreme People's Procuratorate's interpretation of specific legal issues arising in the course of prosecutorial work. Judicial interpretations must be narrowly focused on specific legal provisions and consistent with the purpose, principles, and original intent of the legislation. In other words, judicial interpretations do not have the authority to create new rules. They can only provide guidance on how a particular law should be applied within the existing legal framework.

Using cybercrime as an example, the specific articles of the Chinese Criminal Law prohibiting cybercrime all contain the phrase "With Serious Circumstances [情节严重]."[253] However, the Criminal Law's provisions do not provide a clear definition of what constitutes a serious circumstance accompanying a criminal act or consequence. Assume there is no judicial interpretation defining the criteria for determining whether or not a situation is serious. In that case, no uniform standard exists for judicial organs to follow when applying the law to pertinent cases. As a result, a precise clarification in judicial interpretation is necessary. On the one hand, such issues arise in the application of laws in detail, and it is more convenient for the Supreme People's Court and the Supreme People's Procuratorate to interpret them. If, on the other hand, such issues are reported to the Standing Committee for clarification, it might result in two negative consequences, because legal

[251] PITMAN B. POTTER: The Chinese Legal System: Continuing Commitment to the Primacy of State Power. *The China Quarterly*, vol. 159. (1999) 673-683; PITMAN B. POTTER: *The Chinese Legal System: Globalization and Local Legal Culture*. London, Routledge, 2001, p. 37.

[252] See. GUOYING SHU, 2019, pp. 240-241.

[253] See. Chapter II-2.2

interpretations have the same validity as laws: first, because the procedures for promulgating legal interpretations are different (the Standing Committee's procedures to make legislative interpretations are more stringent), it is unable to respond timely to the requirements of laws' application; second, it is less flexible and thus unable to adapt to the new situation of criminal development and change in a timely manner.[254]

Meanwhile, to ascertain whether something is a source of law and how it operates precisely within a particular legal system, one must examine how judges within that system justify their decisions.[255] In China, both criminal and civil judgments shall cite laws, legal interpretations or judicial interpretations.[256] It means that judicial interpretations are justifications for judges' adjudicating in addition to the laws. Notwithstanding the fact that judicial interpretations have certain prominences, they are neither a formal nor informal source of law. They are merely instructions on how the law should be applied. Although more scholars in China recognize that the line between judicial interpretation and legislation is becoming increasingly blurred, judicial interpretation continues to play a significant role in China's current judicial practices.[257]

To summarize, this section discussed the legal system and the source of law in China. As far as cybercrime governance is concerned, the next sections will introduce cyber policies, cyber law, and cybercriminal law as legal means against cybercrime. Especially with consideration of cybercrime will be dealt with in criminal proceedings, and the criminal judgments could only cite laws and legal and judicial interpretations, the next sections will mainly focus on laws and judicial interpretations. As for the administrative regulations and departmental rules on cyberspace governance, they will be summarized and introduced as

---

[254] See. GUOYING SHU, 2019, pp. 241-243

[255] FÁBIO P. SHECAIRA, 2013, p. 15.

[256] See. Article 3 of the *Provisions of the Supreme People's Court on Citation of Such Normative Legal Documents as Laws and Regulations in the Judgments* [最高人民法院关于裁判文书引用法律、法规等规范性法律文件的规定]: A criminal judgment shall cite laws, legal interpretations or judicial interpretations. Article 4 of these Provisions shall apply to the citation of normative legal documents in judgments of civil suits collateral to criminal proceedings [刑事裁判文书应当引用法律、法律解释或者司法解释。刑事附带民事诉讼裁判文书引用规范性法律文件，同时适用本规定第四条规定]; Article 4 of the *Provisions of the Supreme People's Court on Citation of Such Normative Legal Documents as Laws and Regulations in the Judgments* [最高人民法院关于裁判文书引用法律、法规等规范性法律文件的规定]: A civil judgment shall cite laws, legal interpretations or judicial interpretations, and may directly cite the administrative regulations, local regulations, or regulations on the exercise of autonomy and separate regulations that should be applied [民事裁判文书应当引用法律、法律解释或者司法解释。对于应当适用的行政法规、地方性法规或者自治条例和单行条例，可以直接引用].

[257] See. WENXIAN ZHANG, 2011, pp. 87-88.

context information in the appendix.

2. CYBER-POLICIES IN CHINA

China's policy against cybercrime can be understood from the macro and micro levels.

2.1 THE MACRO LEVEL

The macro aspect of China's policy to deal with cybercrime is not just limited to cybercrime itself. In other words, a more concrete expression of China's macro policy should be its cyber policy. Moreover, the problem of cybercrime is only one part of the governance system of cyberspace. To accurately grasp the Chinese government's cybercrime policy, we have first to sort out China's cyberspace governance policy. The core content of China's cyberspace governance policy can be summarized as the following three points:

First, cyberspace governance[258] should be integrated with comprehensive social governance. Chinese leader Xi Jinping mentioned the concept of an "Internet governance system" in his speech at the first World Internet Conference in 2014.[259] At the same time, in 2019, the fourth Plenary Session of the 19th Central Committee of the Communist Party of China (CPC), the ruling party of China, again emphasized the goal of the Chinese

[258] The term 'Cyberspace' first appeared in the late 1960s. At first, the cyberspace was just on managing the space. It had no connections with something digital, and space here was concrete and physical. [See. JACOB LILLEMOSE AND MATHIAS KRYGER: *The (Re)invention of Cyberspace*. Kunstkritikk, 5 November 2018, https://kunstkritikk.com/the-reinvention-of-cyberspace/] By the using of the Internet, networking and digital communication growing dramatically, the cyberspace started to represent something new related to the Internet. [See. LANCE STRATE: The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, vol. 63. no. 3. (1999) 382-412.] There is an official definition of the Cyberspace which is made by the National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 in the United States that the Cyberspace is "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." [See. The White House. *National Security Presidential Directive 54/Homeland Security Presidential Directive 23*. Cybersecurity Policy. 2008. DOCID: 4123697.] According to this definition, the cyberspace is a kind of virtual environment where people communicate and interact with each other. [See. JANINE KREMLING AND AMANDA M. SHARP PAKER: *Cyberspace, Cybersecurity, and Cybercrime*. SAGE Publications, 2017.] This dissertation agrees with the definition that the cyberspace is the virtual environment based on the Internet and the local area network, the system, and some applications thereof. In this part, the cyberspace is, generally, the Internet environment somehow. It consists of the physical devices, such as the computers, wires, routers and so forth; the provided services online, for example, search engine; the information or data existed in the creation and distribution between the users; and the users.

[259] XINHUANET*: Xi Jinping delivered a congratulatory speech to the first World Internet Conference* [习近平向首届世界互联网大会致贺词]. *World Internet Conference*, 4 November 2021, https://2019.wicwuzhen.cn/web19/wlqg/zwln/201908/t20190822_10862142.shtml

government to establish and improve the comprehensive network governance system.[260] It is worth noting that the theme of the fourth Plenary Session of the 19th CPC Central Committee was to uphold and improve socialism with Chinese characteristics and modernize China's system and capacity for governance. Therefore, China has incorporated cyberspace governance into its national governance system (or comprehensive social governance). This macro policy shows that China has fully recognized the necessity and urgency of (a) governance of cyberspace. Cyberspace governance is an important part of modernizing China's governance system and capacity (the ruling capacity of the CPC); (b) the impact of the development of the Internet on modern social life. The Internet has penetrated every aspect of social life. Cyberspace governance is unavoidable and must be actively addressed; (c) cyberspace governance cannot simply rely on a single instrument of governance, such as the law. Cyberspace governance must be treated like other social issues, and a wealth of policy instruments must be adopted to achieve governance goals.

Second, cyberspace governance requires international cooperation that respects cyber sovereignty. Cyberspace governance requires international cooperation, which does not need to be explained too much. The focus of this policy is on how to understand cyber sovereignty in a Chinese context. The term "cyber sovereignty" refers to the extension of the physical world's concept of sovereignty into cyberspace. It describes the desire of governments to exercise control over the Internet within their own borders, including political, economic, cultural, and technological activities.[261] However, whether sovereignty can adapt to the challenges of cyberspace governance is one of the key questions during the discussion of the issues.[262] The primary impediment to maintaining sovereignty in broad governance issues, including cyber security, is that the rise of non-state actors has resulted in acrimonious conflict with the application of traditional international law based on the rule of sovereignty in these new areas.[263] Some argue that because cyberspace is different from traditional

[260] CENTRAL COMMITTEE OF THE COMMUNIST PARTY OF CHINA: *Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Upholding and Improving the Socialist System with Chinese Characteristics and Promoting the Modernization of the National Governance System and Governance Ability* [中共中央关于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化若干重大问题的决定] Xinhua News Agency, 4 November 2021, http://www.xinhuanet.com/2019-11/05/c_1125195786.htm

[261] See. PAVAN DUGGAL: *Cyber Sovereignty & Cyberlaw*. Independently Published, 2018.

[262] See. YI SHEN: Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, vol. 1. no. 1. (2016) 81-93.

[263] See. STEPHEN D. KRASNER: Abiding Sovereignty. *International Political Science Review*, vol. 22. no. 3. (2011) 229-251.

physical space, the principle of sovereignty cannot be applied to this space shared by all humankind. [264] Additionally, there is an argument that a new global civil society is forming in cyberspace, and that cyber conflicts and wrongdoing have their own mechanisms for resolution. Cyberspace is free from sovereign interference, and the question of how to define the state in a realm devoid of physical boundaries is contentious.[265] However, a number of states, including the Netherlands, France, Austria, the Czech Republic, and Iran, have stated that they believe that an unauthorized cyber incursion into another state by one state could result in a violation of state sovereignty in certain circumstances.[266] China has advocated respect for cyber sovereignty on several occasions. In July 2014, President Xi Jinping issued an official call for countries to respect one another's cyber sovereignty[267], reiterating the point at China's 2015 World Internet Conference.[268] In 2019, China submitted a working paper to the United Nations' Open-ended Working Group (OEWG). In that working paper, China suggested that OEWG should enrich and elaborate on how the principle of sovereignty applies in cyberspace.[269] In the context of domestic China, cyber sovereignty, what the Chinese state advocates, is the collective right to self-determination and development in the face of global structural imbalance.[270]

The third is to maintain network security as the core and protect citizens' legitimate rights and interests. "Without cybersecurity, there can be no national security."[271] "National

---

[264] See. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011)*. White House Policy Document, 22 March 2022, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[265] See. DAVID G. POST: *In Search of Jefferson's Moose: Notes on the State of Cyberspace*. New York, Oxford University Press, 2009.

[266] See. HARRIET MOYNIHAN: The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace. *Journal of Cyber Policy*, vol. 6. no. 3. (2021) 394-410.

[267] See. *Xi Jinping's speech at the National Congress of Brazil (Brasilia, 16 July 2014)* [习近平在巴西国会的演讲]. Xinhua News Agency, 22 March 2022, http://www.xinhuanet.com/world/2014-07/17/c_1111665403.htm

[268] See. XINHUANET: *Xi Jinping delivered a congratulatory speech to the first World Internet Conference* [习近平向首届世界互联网大会致贺词]. World Internet Conference, 4 November 2021, https://2019.wicwuzhen.cn/web19/wlqg/zwln/201908/t20190822_10862142.shtml

[269] See. United Nations. *China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 March 2022, https://front.un-arm.org/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf

[270] See. YU HONG AND ERIC HARWIT: China's Globalizing Internet: History, Power, and Governance. *Chinese Journal of Communication*, vol. 13. no. 1. (2020) 1-7.

[271] See. *Xi Jinping speaks at the first meeting of the Central Internet Security and Informatization Leading Group in Beijing on 27 Feb 2014* [2014 年 2 月 27 日，习近平在中央网络安全和信息化领导小组第一次

cyber security work should adhere to the principle that cyber security is for the people and depends on the people, safeguard personal information security and safeguard citizens' legitimate rights and interests in cyberspace."[272] It can be said that the fundamental goal of China's cyberspace governance is to maintain cyber security. The Chinese government has upgraded cyber security to the same level as safeguarding national security. It shows that the basic logical premise of a series of policy and legal means of cyberspace governance in China is to maintain cyber security. Although protecting citizens' legitimate rights and interests to participate in the Internet is essential to realizing cyber security, the logical focus of China's macro policy of cyberspace governance is still to maintain cyber security. This policy orientation will inevitably face a balance between maintaining cyber security and protecting citizens' legitimate rights and interests in practice. Furthermore, the emphasis on the macro policy will make this balance show a bias. The problem of inclination will be discussed in the following part of this dissertation.

2.2 The Micro Aspects

As mentioned above, China's cyberspace governance policy can be understood as a macro policy to deal with cybercrimes. The micro policies to deal with cybercrimes are specific policies adopted by China under the guidance of macro policies. The content or characteristics of China's micro policies to deal with cybercrimes can be summarized as the following three points:

First, is the crackdown on cybercrimes. "The Internet is not an outlaw place."[273] "We will severely crack down illegal and criminal activities such as cyber hacking, telecom, and cyber fraud, and infringement of citizens' privacy under the law. We also will cut off the chain of interests of cybercrimes and maintain a posture of high pressure to protect the legitimate rights and interests of the people."[274] China's criminal policy on cybercrime is a severe crackdown. It should be noted that the logical center of gravity of policy is "severe."

会议上强调], 4 November 2021, http://www.cac.gov.cn/2019-10/19/c_1573013742660047.htm

[272] See. *In September 2019, Xi Jinping gave important instructions for the National Cybersecurity Publicity Week* [2019 年 9 月，习近平对国家网络安全宣传周做出重要指示强调]. 4 November 2021, http://www.cac.gov.cn/2019-10/19/c_1573013742660047.htm

[273] XUEERSHIXI: *Xi Jinping: The Internet is not a place outside the law* [习近平：互联网不是法外之地]. QSTHEORY.cn, 4 November 2021, http://www.qstheory.cn/zhuanqu/2021-10/13/c_1127952040.htm?ivk_sa=1023197a

[274] See. *Xijinping, president of the communist party of China (CPC), speaks at the national cybersecurity and informatization work conference in Beijing, 20 April 2018* [2018 年 4 月 20 日在全国网络安全和信息化工作会议上的讲话]. 4 November 2021, http://xitheory.china.com.cn/2021-10/13/content_77806480.html

This policy of cracking down on cybercrime is reflected in the work of China's court system. China's Supreme People's Court has mentioned the need to severely punish online crimes in its work highlights for 2018, 2019, and 2020.[275]

Meanwhile, the Supreme People's Court of China's report on strengthening criminal trials in 2019 also mentioned the strict punishment of new types of crimes such as telecommunications networks.[276] According to the theory of criminology, the response to crime should not be limited to punishment but also include prevention, control, and correction. Nevertheless, China's response to cybercrime has been more punitive -- harsh. By nature, it is more likely to be a special deterrent after the fact.

Second, protect women and children's Internet participation. The so-called protection of women and children online participation refers to the legislative and judicial means to improve the legal and regulatory system to protect women and adolescents and severely punish online crimes against women and adolescents. Regarding improving the legal system to protect women and adolescents, China's law on protecting women's rights and interests further strengthens the legislative provisions prohibiting infringement of women's legitimate rights and interests on the Internet.[277] China's Law on the Promotion of Family Education and the Law on the Prevention of Juvenile Delinquency explicitly prevent minors from being addicted to the Internet.[278] Meanwhile, China strictly limits the time that online game enterprises can provide online game services to minors to protect against addiction.[279] In

---

[275] See. SUPREME PEOPLE'S COURT OF CHINA: *Circular of the Supreme People's Court on printing and distributing the Main Points of Work of People's Courts in 2018* [最高人民法院关于印发《2018 年人民法院工作要点》的通知]. 8 February 2018; SUPREME PEOPLE'S COURT OF CHINA: *Circular of the Supreme People's Court on printing and distributing the Main Points of Work of People's Courts in 2019* [最高人民法院关于印发《2019 年人民法院工作要点》的通知]. 24 January 2019; SUPREME PEOPLE'S COURT OF CHINA: *Circular of the Supreme People's Court on printing and distributing the Main Points of Work of People's Courts in 2020* [最高人民法院关于印发《2020 年人民法院工作要点》的通知]. 3 February 2020.

[276] See. SUPREME PEOPLE'S COURT OF CHINA: *Report of the Supreme People's Court on strengthening the work of criminal trials* [最高人民法院关于加强刑事审判工作的报告]. 23 October 2019.

[277] See. Article 42 of the *Law of the People's Republic of China on the Protection of Rights and Interests of Women* [中华人民共和国妇女权益保障法]

[278] See. Article 22 and Article 25 of the *Family Education Promotion Law* [中华人民共和国家庭教育促进法]; Section 5 of the *Law on the Protection of Minors* [中华人民共和国未成年人保护法]; Article 28 of the *Law on the Prevention of Juvenile Delinquency* [中华人民共和国预防未成年人犯罪法].

[279] See. NATIONAL PRESS AND PUBLICATION ADMINISTRATION OF CHINA [国家新闻出版署]: *Notice on Further Strict Management and Preventing Minors from Indulging in Online Games* [关于进一步严格管理切实防止未成年人沉迷网络游戏的通知], 30 August 2021, https://baijiahao.baidu.com/s?id=1710843964825750410&wfr=spider&for=pc

terms of reducing the risk of women and adolescents becoming victims of cybercrimes, especially teenagers,[280] China has used administrative orders and governmental documents to restrict minors from "rewarding" anchors on live streaming services and to strengthen the responsibility of online platforms to reduce the chance that minors become victims of online crimes.[281] In terms of severely punishing online crimes against women and adolescents, China's Supreme People's Court points out that the punishment according to the law for all kinds of serious violent crimes, multiple property crimes as well as to endanger the safety of the food and drug crime, to punish violations left-behind women and children, endanger the safety of campus security, breach of public transportation, telecommunications cyber fraud and other crimes, resolutely safeguard the safety of people's lives and property.[282] At the same time, China's Supreme People's Court has included non-physical indecency crimes committed through the Internet into the category of cybercrimes to be severely cracked down on, thus strengthening the protection of minors.[283]

Third, to serve economic and social development and national economic plans. One of China's cybercrime control goals is to help economic and social development and national economic strategies. Conversely, China's economic and social development and the implementation of the national economic plan demand and require the governance of cybercrimes. In terms of the latter, China's 13th and 14th Five-Year plans for national economic and social development have mentioned the need to play the positive role of Internet technology in the country's economic and social development. The Digital China Development Report released by the Cyberspace Administration of China (CAC) also summarizes the continuous optimization of China's informatization development environment while implementing the 13th Five-Year Plan, including improving cyber laws

[280] *People born after 1990 are the main victims of telecom and Internet fraud* ["90 后" "00 后"成电信网络诈骗主要受害群体], 4 November 2021 http://digital.china.com.cn/2021-08/30/content_41658840.htm (China's Shanghai Municipal Public Security Bureau revealed that the number of victims born after 1990 accounted for more than 60% of the total number of victims of telecom and Internet fraud.)

[281] See. STATE ADMINISTRATION OF RADIO, FILM AND TELEVISION [国家广播电视总局]: *Notice of National Radio and Television Administration on Strengthening management of Online Live Shows and E-commerce Live Shows* [国家广播电视总局关于加强网络秀场直播和电商直播管理的通知], 24 November 2020, http://finance.people.com.cn/n1/2020/1124/c1004-31941750.html

[282] See. SUPREME PEOPLE'S COURT: *Circular of the Supreme People's Court on printing and distributing the Main Points of Work of People's Courts in 2020* [最高人民法院关于印发《2020 年人民法院工作要点》的通知]. 3 February 2020.

[283] See. SUPREME PEOPLE'S COURT: *The Supreme People's Court issued ten outstanding cases on protecting the rights and interests of minors* [最高人民法院发布 10 起利用互联网侵害未成年人权益的典型案例], 31 May 2019.

and regulations and the severe crackdown on cybercrimes.[284] On the former, China's Supreme People's Court reported that the court in China's Jiangsu province realized the crackdown of cybercrime and served the economic and social development goals by hearing cases of the online sales of poisonous and harmful drugs.[285]

3. CYBERLAW IN CHINA

Cyberlaw is an umbrella term of a series of laws or norms on the Internet. Since the 1990s, due to the popularization of the Internet and the apparent infiltration of social production and life caused by the problems, some scholars have gradually paid attention to the study of cyberlaw.[286] Throughout the study of cyberlaw, the name of cyberlaw is changing and developing. The differences of cyberlaw, cyberspace law[287], Internet law[288], information technology law[289], and so on show the scholars' different cognition of cyberlaw or the essential characteristics of the Internet.[290] However, any definition of cyberlaw inevitably involves a keyword: Information technology. Accordingly, this dissertation considers cyber-law as a general term for a series of normative on regulating the adverse effects of information technology and its characteristics on social production and life. This dissertation holds that the definition of cyberlaw can be divided into broad and narrow definitions.

In a broad sense, cyberlaw includes laws dealing with the Internet and cases, regulations, rules, and disputes arising from interaction with information technology that affects people's social production and life.[291] In the case of China, the broad aspect of

---

[284] CYBERSPACE ADMINISTRATION OF CHINA (CAC): *Cyberspace Administration of China (CAC) releases Digital China Development Report 2020* [国家互联网信息办公室发布《数字中国发展报告（2020 年）》], 3 July 2021, http://www.gov.cn/xinwen/2021-07/03/content_5622668.htm

[285] See. SUPREME PEOPLE'S COURT: *Judicial report on the People's Courts serving and safeguarding the integrated development of the Yangtze River Delta* [人民法院服务和保障长三角一体化发展司法报告], 2 November 2021.

[286] See. e.g., JONATHAN ROSENOER: *CyberLaw: The Law of the Internet*. New York, Springer, 1997; LAWRENCE LESSIG: The Path of Cyberlaw Symposium: Emerging Media Technology and the First Amendment. *Yale Law Journal*, vol. 104. no. 7. (1995) 1743-1756.

[287] See. e.g., KRIANGSAK KITTICHAISAREE: Public International Law of Cyberspace. Switzerland, Springer, 2017.

[288] See. e.g., JOSEPH SAVIRIMUTHU: Rethinking Cyberlaw: A New Vision for Internet Law Book Review. *SCRIPTed: Journal of Law, Technology and Society*, vol. 13. no. 3. (2016) 393-397.

[289] See. e.g., CHRIS REED: Introduction. In: CHRIS REED (ed): *Computer Law*. Oxford University Press, 2011. iv-iviii.

[290] See. ITSUKO YAMAGUCHI: Cyberlaw. *Theory, Culture & Society*, vol. 23. no. 2-3. (2006) 529-531.

[291] See. BRAIN CRAIG: *Cyberlaw: The Law of the Internet and Information Technology*. United States,

China's cyber-law introduced and studied in this dissertation includes not only laws explicitly directed at Internet technology, cybersecurity, and management of cyberspace, but also provisions concerning information networks scattered among laws of other departments, such as civil law, commercial law and social law. Compared with the broad concept of cyberlaw, the narrow definition only includes those laws specifically aimed at the Internet. The narrow definition of China's cyber-law adopted in this dissertation only consists of those laws enacted by the National People's Congress of the People's Republic of China (NPC) and its Standing Committee (NPC-SC). It is worth noting that the very concept of cyberlaw is controversial. The novelty of the problems solved by cyberlaw does not come from the fact that the issues themselves are new but from the alienation of traditional inherent problems based on the popularization and development of Internet technology.[292] For example, cyberlaw addresses free speech, intellectual property, privacy, security, and e-commerce, which are prominent and inherent normative areas of the Constitution, Copyright Law, and Commercial Law. Therefore, some scholars criticize whether network law itself is a new field of law worthy of independence.[293] However, although such criticism is instructive for the reflection of the study of cyber-law, it does not prevent this dissertation from taking cyber-law as a kind of classification standard to summarize and sort out China's Internet legislation. To sum up, in the following part, this dissertation will summarize China's cyber-laws from the perspective of broad and narrow definitions and briefly comment on them.

3.1 THE NARROW DEFINITION OF CYBERLAW IN CHINA

On 28 December 2000, the 19th Session of the Standing Committee of the Ninth National People's Congress adopted the *Decision of the Standing Committee of the National People s Congress on Preserving Computer Network Security* [全国人大常委会关于维护互联网安全的决定] (after this referred to as the Decision).[294] The legislative background of the

Pearson, 2012. p. 2.

[292] See. RORY MCLNTYRE-O'BRIEN: Is There Such a Thing of Cyberlaw. *Irish Student Law Review*, vol. 11. no. (2003) 118-129.

[293] See. JOSEPH H. SOMMER: Against Cyberlaw. *Berkeley Technology Law Journal*, vol. 15. no. 3. (2000) 1145-1232.

[294] The Decision was amended once in *the Provisions on Revising Some Laws* [全国人大常委会关于修改部分法律的决定] adopted at the 10th Session of the 11th National People's Congress Standing Committee on 27 August 2009. The Provisions on Amending Some Laws in 2009 amended Article 6 of the decision, changing the original Article 6 "Regulations on Public Security Administration Penalties [治安管理处罚条例]" into "Law on Public Security Administration Penalties [治安管理处罚法]." The revision in 2009 was a formal one, which mainly unified the appellation of the legal system and did not involve any substantive revision.

Decision is that the influence of the Internet in China's economic construction and social undertakings on the profound changes in social production and life must be regulated by specific laws. The Decision has seven parts, covering the use of the Internet to threaten national security, economic order, social order, Internet operation security, legal rights of individuals, criminal penalties, non-criminal penalties, and government responsibilities. The main characteristics of the Decision are as follows:

(a) the criminal law as the primary means to regulate cybercrime;

(b) extensive use of expressions such as "in violation of state regulations," even though most state regulations relating to the Internet were not established in the legal form at the time;

(c) it initially reflects the policy of comprehensive Internet governance, that is, in addition to Criminal Law, Civil law, and other legal methods, strengthening publicity and education and the implementation of adequate supervision and management are also written into the Decision.

On 7 November 2016, the 24th Session of the Standing Committee of the 12th National People's Congress of China adopted *the Cybersecurity Law of the People's Republic of China* [中华人民共和国网络安全法] (after this referred to as the Cybersecurity Law). The Cybersecurity Law is China's first law specialized in cybersecurity to regulate activities in cyberspace. The Cybersecurity Law took effect on 1 June 2017. The Cybersecurity Law consists of seven chapters. In addition to the general provisions of Chapter 1 and supplementary provisions of Chapter 7, the other five chapters respectively provide network security support and promotion, network operation security, network information security, monitoring and early warning and emergency response, and legal liability. As the first relatively mature cyberlaw, the "cybersecurity" theme of the Law shows that China's cyberspace governance focuses on maintaining network security policy. The Cybersecurity Law stipulates the real-name system on the Internet and international cooperation in combating cybercrime.[295] The Cybersecurity Law also initially requires Internet enterprises or network operators to protect citizens' personal information.[296]

To regulate the business activities of selling goods or providing services through the Internet and other information networks, the Standing Committee of the 13th National

[295] See. Article 24 of the *Cybersecurity Law*.

[296] See. Chapter VI of the *Cybersecurity Law*: Legal Liability.

People's Congress of China adopted and promulgated the *E-commerce Law of the People's Republic of China* [中华人民共和国电子商务法] (after this referred to as the "E-commerce Law") on 31 August 2018. The E-commerce Law took effect on 1 January 2019. With the development of Internet technology, online shopping and other behaviors are increasingly popular in China and have a profound impact on the daily life of Chinese people.[297] To regulate the buying and selling behaviors in the Internet and other information network space. E-commerce law clearly defines a series of concepts, such as e-commerce operators, e-commerce platform operators, etc. At the same time, E-commerce Law stipulates the content of e-commerce contracts, which makes up for the deficiency of traditional contract law in cyberspace application.

It is worth mentioning that China is considering a law to curb telecom and Internet fraud. The 31st Session of the Standing Committee of the 13th National People's Congress of China deliberated the *Anti-Telecommunications Network Fraud Law of the People's Republic of China (the Draft)* [中华人民共和国反电信网络诈骗法（草案）] (after this referred to as the "Draft"). At present, the Draft is still in the public consultation process, has not been formally adopted. The Draft considers the increasingly high incidence and great harm of the current situation of telecom network fraud, plans to prevent and control the telecom network fraud and cybercrime through special legislation. The Draft emphasizes the Internet real-name system[298], expressing the positive correlation between the Internet real-name system and cybercrime intervention and prevention.

3.2 THE BROAD DEFINITION OF CYBERLAW IN CHINA

In conjunction with the preceding introduction under a narrow definition of cyberlaw, this section of the introduction and reorganization under a broad definition of cyberlaw will focus on other laws in addition to the aforementioned directions.

---

[297] See. e.g., GUANGMING NET: *Tmall Double 11 calendar year turnover summary* [天猫双 11 历年交易额汇总]. Sohu News, 9 November 2021, https://www.sohu.com/na/431088718_162758 [In 2012, Taobao Mall officially changed its name to Tmall. Online transactions totaled 19.1 billion yuan. The total value of transactions reached 36.2 billion yuan in 2013. In 2014, the transaction volume exceeded 100 million yuan in 74 seconds, and the whole day's transaction volume reached 57.1 billion yuan..... The final transaction volume in 2015 reached 91.217 billion yuan. In 2016, the 24-hour total turnover reached 120.7 billion yuan, with 175,000 transactions per second at its peak. In 2017, the total turnover reached 168.2 billion yuan. In 2018, the final transaction value reached 213.5 billion yuan, breaking the 200 billion marks for the first time. In 2019, the turnover in 14 seconds exceeded 1 billion yuan, with a total turnover of 268.4 billion yuan. From 0 o'clock on November 1, 2020 to 0 o'clock on November 11, 2020, the real-time transaction volume of Tmall shopping carnival on November 11 exceeded 372.3 billion yuan.]

[298] See. Article 7 of the *Draft*.

In terms of maintaining cybersecurity and national security, except the Decision and Cybersecurity Law, the Standing Committee of the National People's Congress of China has also regulated the challenges posed by the Internet and other information networks and their responses to them in other laws. They included but were not limited to:

(a) The *Counterterrorism Law of the People's Republic of China* [中华人民共和国反恐怖主义法] (after this referred to as the "Counterterrorism Law") was enacted to combat terrorism. The Counterterrorism Law was promulgated and came into force on 27 April 2018. Article 19, 84, and 86 of the Counterterrorism Law stipulate telecom business operators' duty, responsibility, and punishment in anti-network terrorism.

(b) The *Cryptography Law of the People's Republic of China* [中华人民共和国密码法] (after this referred to as the "Cryptography Law") was formulated to standardize the application and management of passwords and ensure network and information security. The Cryptography Law was promulgated on 26 October 2019 and took effect on 1 January 2020.

(c) The *Law of the People's Republic of China on Guarding State Secrets* [中华人民共和国保守国家秘密法] (after this referred to as the "Law on Guarding State Secrets") was enacted to guard State Secrets. The Law on Guarding State Secrets was passed on 5 September 1988 and revised at the 14th Session of the 11th National People's Congress of China on 29 April 2010. The revised Law on Guarding State Secrets came into force on 1 October 2010. Articles 24, 26 to 28, and 50 of the revised Law on Guarding State Secrets have been added to regulate and restrict the disclosure of state secrets through the Internet and other information networks, and the acts of violation that put state secrets at risk, as well as the legal liabilities and penalties for such actions.

The NPC has adopted the *Civil Code of the People's Republic of China* [中华人民共和国民法典] (after this referred to as the "Civil Code") to protect citizens' rights of the person and property. The Civil Code was promulgated on 28 May 2020 and entered into force on 1 January 2021. Article 1028, 1194 to 1197 of the Civil Code established general rules for civil subjects dealing with infringements on the Internet.

As far as intellectual property rights protection is concerned, the NPC-SC amended

the *Copyright Law of the People's Republic of China* [中华人民共和国著作权法] (after this referred to as the "Copyright Law") on 11 November 2020 and took effect on 1 June 2021. The newly revised Copyright Law mainly stipulates copyright protection in cyberspace and the acts and legal liabilities of infringing copyright by using information networks.

In terms of protecting citizens' personal information, the Standing Committee of the National People's Congress of China had formulated the *Personal Information Protection Law of the People's Republic of China* [中华人民共和国个人信息保护法] (after this referred to as the "Personal Information Protection Law"). The Personal Information Protection Act was promulgated on 20 August 2021 and took effect on 1 November 2021. Article 4 of the Personal Information Protection Law defines personal information as all kinds of information recorded electronically or in other ways related to identified or identifiable natural persons, excluding the information after anonymization. Among them, electronic information is mainly generated in cyberspace, such as the Internet. Therefore, the personal information protection law can be regarded as one of the components of the general cyberlaw. On the other hand, the Cyberspace Administration is the main administrative responsible organ stipulated in the Personal Information Protection Law, reflecting the cyberlaw features of the personal information protection law.

In terms of protecting the rights and interests of minors and preventing juvenile crimes, the NPC-SC has enacted:

(a) The *Law of the People's Republic of China on the Protection of Minors* [中华人民共和国未成年人保护法] (after this referred to as the "Law on the Protection of Minors"). The Law on the Protection of Minors was amended on 17 October 2020 and came into force on 1 June 2021. The revised Law on the Protection of Minors in 2020 added a particular chapter, Chapter 5, to protect minors on the Internet, including regulating online dissemination of obscenity, pornography, violence, cult, superstition, gambling, and illegal publications of other online information.

(b) The *Law of the People's Republic of China on the Prevention of Juvenile Delinquency* [中华人民共和国预防未成年人犯罪法] (after this referred to as the "Law on the Prevention of Juvenile Delinquency"). The Law on the Prevention of Juvenile Delinquency was promulgated on 26 December 2020 and entered into force on 1 June 2021. Article 28 of the Prevention of Juvenile Delinquency Act regards juvenile addiction to the Internet as a deviant behavior regulated by the Act.

(c) The *Law of the People's Republic of China on Family Education Promotion* [中华人民共和国家庭教育促进法] (after this referred to as "Family Education Promotion Law"). The Family Education Promotion Law was promulgated on 23 October 2021 and will take effect on 1 January 2022. Article 22 of the Family Education Law specifies the need to prevent minors from indulging in deviant behavior on the Internet.

It is worth mentioning that on 7 December 2020, China's National Radio and Television Administration issued the *Notice on Strengthening Management of Online Show Live Broadcast and E-commerce Live Broadcast* [国家广播电视总局关于加强网络秀场直播和电商直播管理的通知], strictly restricting minors' "reward" behavior in an online live broadcast. On 30 August 2021, China's National Press and Publication Administration issued a *Notice of Further Imposing Strict Administrative Measures to Prevent Minors from Becoming Addicted to Online Games* [国家新闻出版署关于进一步严格管理切实防止未成年人沉迷网络游戏的通知], strictly limiting the time when online game services can be provided to minors. All online game enterprises can only offer one hour of service on Friday, Saturday, Sunday, and statutory holidays to minors from 20:00 to 21:00 a day.

In terms of standardizing the dissemination of online culture and the operation of online media, on 29 April 2021, the NPC-SC revised the *Advertising Law of the People's Republic of China* [中华人民共和国广告法] (after this referred to as the "Advertising Law") and published the *Anti-food Waste Law of the People's Republic of China* [中华人民共和国反食品浪费法] (after this referred to as "Anti-food Waste Law").

Article 40 of the revised Advertising Law stipulates those advertisements of online games detrimental to minors' physical and mental health shall not be disseminated on the Internet and other mass media. Article 44 of the revised Advertising Law stipulates that the use of the Internet to publish advertisements shall not affect the regular use of the Internet. Article 22 of the Anti-food Waste Law specifies that information about wasted food cannot be produced, published, or disseminated on the Internet.

To maintain market order and promote social and economic development, the NPC-SC:

(a) amended the *Law of the People's Republic of China on the Protection of Consumer Rights and Interests* [中华人民共和国消费者权益保护法] (after this

referred to as the "Consumer Protection Law") for the second time on 25 October 2013. The second amendment to the Consumer Protection Law stipulates that consumers can return goods purchased through the information network within seven days; operators using the information network must provide essential information to consumers. To a certain extent, the second amendment of the Consumer Protection Law regulates the business behavior of operators who use the Internet and other information networks, responds to the dilemma of consumer rights protection faced by the booming online shopping in China, and further promotes the development of Internet economy.

(b) amended the *Anti-Unfair Competition Law of the People's Republic of China* [中华人民共和国反不正当竞争法] (after this referred to as the "Anti-Unfair Competition Law") on 23 April 2019. The amendment to the Anti-Unfair Competition Law mainly includes the use of the Internet and other information network technologies to conduct the malicious competition in the scope of jurisdiction, further consolidating the positive development trend of China's Internet economy.

(c) amended the *Food Safety Law of the People's Republic of China* [中华人民共和国食品安全法] (after this referred to as the "Food Safety Law") on 29 April 2021. The amendments to the Food Safety Law mainly regulate Internet platforms for food business and strengthen the management responsibility of online food trading platforms. The amendments to the food safety law respond to the turmoil in China's rapidly growing online food delivery market and aim to regulate the market order of online food transactions.

For more information about cyberlaw in administrative regulations and departmental rules, please see Appendix I and Appendix II.

4. CYBERCRIMINAL LAW IN CHINA

Criminal law is the law prescribing crime, criminal responsibility, and punishment. Criminal law has a broad and narrow definition. In a broad sense, criminal law refers to the sum of all the provisions of crime, criminal responsibility, and criminal law. It mainly includes criminal code, separate criminal law, and subsidiary criminal law. In the narrow sense, criminal law refers to the criminal code that systematically stipulates crime, criminal

responsibility, and penalty. It is only one of the contents of the broad criminal law.[299] The cyber-criminal law discussed in this part, combined with the basic definition of criminal law, refers to the laws and regulations prescribing cybercrimes and their criminal responsibility and penalties. This part of the cyber-criminal law is based on the definition of criminal law in the broad sense and made a certain expansion. Specifically, the cyber-criminal law in this dissertation includes provisions on cybercrimes in China's Criminal Code and its amendments. It also includes judicial interpretations of these provisions made by China's Supreme People's Court (SPC) and Supreme People's Procuratorate (SPP). The purpose of adopting this expansion is to present a relatively complete system of criminal laws and regulations for dealing with cybercrimes in China. In comparison to Chapter II-2.2, this section focuses on the evolution of Chinese criminal law's approach to cybercrime.

4.1 CYBERCRIME IN THE CRIMINAL CODE AND ITS AMENDMENTS

The Criminal Law of the People's Republic of China, which was promulgated in 1979 and revised in 1997, and has been amended several times, is China's Criminal Code. In the Criminal Code of China, the provisions on cybercrime show a trend of gradual development. Due to the times and technology situation, China's 1979 Criminal Law has no provisions on cybercrimes. It was not until 1997, when China revised the criminal Law of 1979, that the provisions of cybercrimes were initially set up, namely, Article 285 (crime of unauthorized intrusion into computer information systems), Article 286 (crime of vandalizing computer information systems) and Article 287 (suggestive provisions of using computers to commit crimes). The focus of Article 285 and Article 286 is different. The former is for the invasion of a specific computer system; the latter is for the destruction of computer information systems (including the production, spread of computer viruses and deleting, modifying the original system data, and other interference with the regular operation of the computer information system). Article 287 expresses a general attitude towards cybercrimes that use computers to carry out traditional crimes, applying the provisions of specific crimes to convict and punish. It should be noted that the crime of illegal intrusion into the computer information system in 1997 only included the unlawful intrusion into the computer information system in the field of state affairs, national defense construction, and cutting-edge science and technology into the scope of punishment, and did not involve other computer information systems such as civil and commercial. But the crime of destroying

[299] CRIMINAL LAW EDITORIAL: *Criminal Law (Volume1: General)* [刑法学（上册・总论）]. Beijing, Higher Education Press, 2019. p. 36.

computer information systems does not limit the property of computer information systems.

On 28 February 2009, the 7th Session of the Standing Committee of the 11th National People's Congress adopted *Amendment (VII) to the Criminal Law of the People's Republic of China* (after this referred to as "Amendment VII"). Article 9 of Amendment VII expands Article 285 of Criminal Law by adding two provisions, including three aspects: first, the computer information system as the object of the crime is extended to other computer information systems besides the original national computer information system; second, the expansion of criminal means, that is, in addition to illegal intrusion, also includes illicit control of computer information system; the third is to criminalize acts of assisting in committing a crime, such as providing criminal programs and tools.

On 29 August 2015, the 16th Session of the Standing Committee of the 12th National People's Congress adopted the *Amendment (IX) to the Criminal Law of the People's Republic of China* (after this referred to as "Amendment IX"). Amendment IX can be a significant reform or progress in dealing with cybercrimes in China's Criminal Code. Specifically:

(1) Article 16 of Amendment IX adds a paragraph as the third paragraph to Article 246 of criminal Law, extending the crime field of insult and defamation to cyberspace and investigating criminal responsibility for insult and defamation through the information network.

(2) Article 28 of Amendment IX adds an article after article 286 of the Criminal Code as article 286 (I). Article 286 (I) specifies the platform responsibilities of the Internet Service Providers. In other words, according to Article 286 (I), when Internet service providers fail to fulfill the obligations of information network security management prescribed by laws and regulations and refuse to adjust after being ordered to rectify by the regulatory authorities, thus causing serious consequences, they shall bear criminal liability. The severe repercussions here include but are not limited to the massive dissemination of illegal information, the disclosure of user information and resulting in serious consequences, and the loss of evidence in criminal cases.

(3) Article 29 of Amendment IX adds two articles after Article 287 of the Criminal Code as Article 287 (I) (crime of illegal utilization of information network technology) and Article 287 (II) (crime of provision of assistance to conduct the cyber-criminal activity). Section 287 (I) provides for three modes of conduct: first is

the establishment of websites and instant messaging groups to establish criminal activity (focusing on the unreasonableness of the establishment of websites and instant messaging groups for criminal activity); second, the release of illegal and criminal information (focusing on the illicit and irrational content of the information itself); the third is to release information for the implementation of criminal and unlawful activities (focusing on the purpose of releasing information illegal and criminal acts and irrationality, information content itself may not have irrationality). Section 287 (II) criminalizes aiding and abetting cybercrime by providing technical support such as Internet access, server hosting, network storage, and communication transmission, or assisting such as advertising, payment, and settlement. Combined with the suggestive provisions of Article 287 of the Criminal Law, it is not difficult to find that Article 287 (I) and Article 287 (II) separately criminalize the preparatory behavior and helping behavior of traditional crimes by using information networks. Accordingly, the offenses defined in Articles 287 (I) and 287 (II) are summarized as Auxiliary Cybercrime.

(4) Article 32 of Amendment IX adds a second paragraph to Article 291 of the Criminal Code. Article 32 criminalizes the behavior of fabricating and spreading false information about dangerous situations, epidemic situations, disasters, and warnings on information networks or knowingly spreading such fake news on information networks and causing severe consequences.

On 24 December 2020, the 24th Session of the Standing Committee of the 13th National People's Congress adopted the *Amendment (XI) to the Criminal Law of the People's Republic of China* (after this referred to as "Amendment XI"). The revision of Amendment XI in dealing with cybercrimes mainly focuses on copyright and copyright-related rights. Article 20 of Amendment XI amended Article 217 of the Criminal Law, the crime of infringing copyright. Its main feature is that copyright infringement extends to cyberspace and is determined by criminal law, reflecting China's Criminal Law protection of copyright to cope with the challenge of information network technology to copyright. Amendment XI made to the copyright infringement crime is in line with the amendment made by the Standing Committee of the National People's Congress to the Copyright Law on 11 November 2020. It shows that both criminal law and copyright law deeply recognize the impact of the Internet and other information networks on copyright protection in China, and it is necessary to realize the network protection of copyright through explicit legislation.

4.2 CYBERCRIME IN THE JUDICIAL INTERPRETATIONS

Sixteen major judicial interpretations of cybercrimes are in force in China, covering pornography crimes, financial crimes, infringement of personal information crimes, auxiliary cybercrime, telecom network fraud crimes, cyber slander, rumors crimes, and gang-related crimes. Most of these judicial interpretations are explicitly designed for cybercrime. Of course, there are a few judicial interpretations whose theme is not specifically for cybercrime but also includes the use of the Internet or in terms of the crime. For example, Article 8 of the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases regarding Organizing, Forcing, Inducing, Sheltering, or Introducing Prostitution* [最高人民法院、最高人民检察院关于办理组织、强迫、引诱、容留、介绍卖淫刑事案件适用法律若干问题的解释] stipulates:

> *„Whoever publishes whoring and other illegal information on the information network, if the circumstances are severe, shall be convicted and punished for the crime of illegal utilization of the information network under Article 287 (a) of the Criminal Law."*

This dissertation reviews the titles, effectiveness, issuing authority, and effective time of these 16 judicial interpretations. (See. Appendix III) By sorting out them, this dissertation briefly summarizes the characteristics of China's judicial interpretations on cybercrime as follows:

First, these judicial interpretations responded positively to the new criminal legislation and the hot issues of cybercrime in Chinese society at that time. For example, article 6 of the *Opinions on Punishing Criminal and Illegal Activities that Hinder the Prevention and Control of Novel Coronavirus Pneumonia* [关于依法惩治妨害新型冠状病毒感染肺炎疫情防控违法犯罪的意见] provide for the legal punishment of fabricating false epidemic information and disseminating it on the Internet, as well as the legal sentence of Internet service providers for failing to fulfill their administrative obligations and refusing to correct after being ordered to do so by relevant authorities, resulting in the dissemination of a large number of false epidemic information.

Second, these judicial interpretations are usually jointly formulated by the Supreme People's Court and the Supreme People's Procuratorate to establish a unified standard for

judicial practice in dealing with cybercrimes. Of the 16 judicial interpretations, the SPP and SPC participated in the formulation of 12, accounting for 75 percent. The SPP alone formulated four, accounting for 25 percent. The judicial interpretation of the four cybercrimes independently made by the SPP mainly concerns the procedural provisions of procuratorial organs in handling cybercrime cases. The judicial interpretation of the substantive provisions on cybercrime is usually jointly formulated by the two departments.

Third, identifying the degree of harm of cybercrime adopts the "qualitative + quantitative" method. "quantity," "frequency," "amount," and other specific quantitative standards are widely used in the provisions of judicial interpretation to judge the seriousness of cybercrimes.[300]

We need to pay attention to or reflect on whether this approach of determining the severity of the case by quantity is too rigid. For example, Article 1 of the *Interpretation on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations* [最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释] stipulates:

> *„In case anyone who makes, reproduces, publishes, sells, or spreads pornographic electronic information for seeking profits by means of the internet or terminal of mobile communications, and has any of the following circumstances, he shall be convicted and punished as the crime of making, reproducing, publishing, selling and spreading pornographic articles for seeking profits in accordance with the provisions of paragraph 1 of Article 363 of the Criminal Law:[4] The pornographic*

[300] See. e.g., Article 1 of the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about the risks of Computer Information Systems* [最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释], Article 2 of the *Interpretation on Several Issues concerning the Specific Application of Law in the Handling of Defamation through Information Networks and Other Criminal Cases* [最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释], and Article 3, Article 10, and Article 12 of the *Interpretations on Several Issues concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to Information Network* [最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释], etc.

electronic information made, copied, published, sold, or spread by him is clicked more than 10 thousand times."

What is the difference between 10,000 hits and 9,999 hits? This over-reliance on the quantitative method seems too rigid in judicial practice and can not sufficiently realize the purpose and significance of criminal law setting related crimes. However, the reliance on "quantitative + qualitative" could not be too blamed for existing lawmaking techniques.

4.3 JUDICIAL JURISDICTION OF CYBERCRIME IN CHINA

Generally, in the field of international law, States have three types of jurisdictional competences, namely, legislative jurisdiction, executive jurisdiction, and judicial jurisdiction. Legislative jurisdiction refers to the authority of the State to enact laws and regulations for a particular matter or conduct. Executive jurisdiction refers to the authority of a State to apply and enforce its laws and norms through administrative acts. Jurisdiction means the competence of a State's national courts to administer disputes before it.[301] In the field of criminal procedure law, judicial jurisdiction refers to the scope of authority and specific division of labor between courts at all levels and between courts at the same level in different regions to accept first-instance criminal cases. As far as cybercrime is concerned, it mainly has two forms of jurisdiction in China: hierarchical jurisdiction and territorial jurisdiction. Hierachical jurisdiction mainly solves the problem of the level of court at which the first-instance cybercrime case is heard. Territorial jurisdiction mainly solves the problem of the court of which place to hear the first-instance cybercrime case.

4.3.1 Hierachical Jurisdiction of Cybercrime in China

China's court system is divided into four levels: the basic people's courts, the intermediate people's courts, the high people's courts, and the Supreme People's Court. As far as the first instance trial of criminal cases is concerned, the basic people's courts have jurisdiction over ordinary criminal cases; the intermediate people's courts have jurisdiction over cases regarding compromising national security or terrorist activities or cases where life imprisonment or death penalty may be imposed; the higher people's courts have jurisdiction over significant criminal cases in the provincial-level region where they are located; and the Supreme People's Court has jurisdiction over significant criminal cases of a nationwide

[301] See. MICHAEL N. SCHMITT AND LILS VIHUL: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. New York, Cambridge University Press, 2017, pp. 51-52.

nature.[302] In fact, China's high people's courts and Supreme People's Court rarely hear criminal cases in the first instance. Therefore, the first instance trial of criminal cases is usually under the jurisdiction of the basic people's courts and intermediate people's courts.

In terms of cybercrime cases, the vast majority of first-instance trials in China are conducted by basic people's courts, in accordance with the principle of hierarchical jurisdiction discussed previously. Only when it comes to the use of information networks to commit crimes involving the compromise of national security or cyber terrorism will they be tried in the intermediate people's courts in the first instance.

4.3.2 Territorial Jurisdiction of Cybercrime in China

Article 25 of China's Criminal Procedure Law establishes the basic principle of judicial jurisdiction over criminal cases, that is, in principle, the people's court at the place where the crime was committed (place of crime [犯罪地]) has jurisdiction over criminal cases; in exceptional cases, the jurisdiction of the people's court at the defendant's resident place [被告人居住地] may be exercised.[303] How to understand *the place of crime* is critical to the proper application of the territorial jurisdiction principle. Is the term place of crime limited to the place of criminal acts or does it include the place of the crime's result? In response to this question, the Supreme People's Court interpreted the place of crime as *the place where the criminal act occurred* through a piece of judicial interpretation in 1998.[304] However, Article 6 of China' Criminal law stipulates that: When either the act or consequence of a crime takes place within P.R.C. territory, a crime is deemed to have been committed within P.R.C. territory.[305] Although this provision discusses the issue of jurisdiction between states, it reflects the understanding of *the place of crime* in China's criminal substantive law.

---

[302] See. Article 20 to 23 of the *Criminal Procedure Law of the People's Republic of China* [中华人民共和国刑事诉讼法]

[303] See. Article 25 of the *Criminal Procedure Law of the People's Republic of China* [中华人民共和国刑事诉讼法]: A criminal case shall be under the jurisdiction of the people's court at the place of crime. Where it is more appropriate for the case to be tried by the people's court at the place of residence of the defendant, the case may be under the jurisdiction of the people's court at the place of residence of the defendant [刑事案件由犯罪地的人民法院管辖。如果由被告人居住地的人民法院审判更为适宜的，可以由被告人居住地的人民法院管辖].

[304] See. Article 2 of the *Interpretation of the Supreme People's Court on the Application of the Criminal Procedure Law of the People's Republic of China (1998)* [最高人民法院关于适用《中华人民共和国刑事诉讼法》的解释 (1998)]. (This piece of judicial interpretation had been expired since 2012.)

[305] See. Chinse version: [犯罪的行为或者结果有一项发生在中华人民共和国领域内的，就认为是在中华人民共和国领域内犯罪].

In order to reconcile this contradiction and to meet the substantial demand of combatting crimes, in 2012, six national organs in China adopted a provision clarifying that: The "place of crime" as mentioned in the Criminal Procedure Law includes the place where a criminal act is committed and the place where a criminal consequence occurs.[306] Supreme People's Court in 2021 further improves the above expression through a new judicial interpretation: The place of crime shall include the place of criminal acts [犯罪行为地] or the place of consequences of crime [犯罪结果地].[307]

The emergence of cybercrime has created significant tensions with the principle of the validity in terms of space of criminal punishment in China, which is based on the principle of territorial jurisdiction.[308] Simultaneously, as criminal offenses and computer networks become more integrated, criminal prosecutions face unprecedented challenges.[309] Due to the concealed, sudden, and cross-regional nature of cybercrime, cybercrime cases are becoming increasingly unsuitable for China's criminal justice system, which is dominated by territorial jurisdiction.[310] Specifically, critical elements of cybercrime, such as websites, communication tools, suspects, victims, and target computers, are frequently dispersed across multiple locations.[311] It is difficult to classify their locations simply as the place of crime or the place of consequence of the crime. However, neither the 2012 nor 2018 revised Criminal Procedure

[306] See. Article 2 of the *Provisions of the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security, the Ministry of Justice, and the Legislative Affairs Commission of the Standing Committee of the National People's Congress on Several Issues concerning the Implementation of the Criminal Procedure Law* [最高人民法院、最高人民检察院、公安部、国家安全部、司法部、全国人大常委会法制工作委员会关于实施刑事诉讼法若干问题的规定]: [刑事诉讼法规定的犯罪地，包括犯罪的行为发生地和结果发生地].

[307] See. Article 2 of the *Interpretation of the Supreme People's Court on the Application of the Criminal Procedure Law of the People's Republic of China (2021)* [最高人民法院关于适用《中华人民共和国刑事诉讼法》的解释 (2021)]: [犯罪地包括犯罪行为地和犯罪结果地].

[308] See. ZESHAN ZHENG: Cybercrime and the Principle of the Validity in terms of Space in Criminal Law [网络犯罪与刑法的空间效力原则]. *Chinese Journal of Law* [法学研究], no. 5. (2006) 71-81.

[309] See. YONGSHENG CHEN: Challenges to Modern Criminal Procedure Brought by Cybercrime and Its Institutional Response [计算机网络犯罪对刑事诉讼的挑战与制度应对]. *Science of Law (Journal of Northwest University of Political Science and Law)* [法律科学(西北政法大学学报)], vol. 32. no. 3. (2014) 140-153; KE-YIN AN: China's Participation in the International Control of Transnational Cybercrime [跨国网络犯罪国际治理的中国参与]. *Journal of Yunnan Minzu University (Social Sciences)* [云南民族大学学报(哲学社会科学版)], vol. 36. no. 3. (2019) 155-160.

[310] See. SHENGBIN TIAN: On the Jurisdiction System of Internet Criminal Cases [互联网刑事案件管辖制度研究]. *Tribune of Political Science and Law* [政法论坛], vol. 39. no. 3. (2021) 36-48.

[311] HAISONG YU: The Recent Development of the Criminal Procedure Rules of Cybercrime: Based on the "Interpretation of the New Criminal Procedure Law" [网络犯罪刑事程序规则的新近发展：基于《新刑事诉讼法解释》的解读]. *China Journal of Applied Jurisprudence* [中国应用法学], no. 5. (2021) 51-61.

Law prescribed the specific application of the jurisdiction of cybercrime. Instead, the specific provisions on the place of cybercrime are mainly determined in the form of judicial interpretations.

In 2016, the judicial interpretation on cyber fraud jointly issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security stipulated that: *The place where the criminal act takes place* shall include the place where a web server used for the crime of telecommunications network fraud is located, the place where the founder or manager of a website is located, the place where the victim computer information system or the manager thereof is located, the place where the computer information system used by criminal suspect or the victim is located, the place where a fraud call, short text message, or e-mail, among others, is made, sent, or received or arrives, and the place where a constant fraud act is committed, prepared, or started, or transits or ends; *The place where the result of a crime takes place* shall include the place where the victim is located when defrauded, and the place where the property obtained by fraud is actually obtained, concealed, transferred, used or sold, among others.[312]

In 2021, the above three organs added the following matters in a new judicial interpretation on cyber fraud: The place of crime of cyber fraud shall also include (1) the places of issue, sale, transfer, and concealment of a SIM card, data SIM card, or IoT SIM cards used for criminal activities; (2) the places of issue, sale, transfer, concealment, and use of a credit card used for criminal activities and the places of cash delivery and remittance by the counterparty in a cash transaction; (3) the places of opening, sale, and use of a bank account or non-bank payment account used for criminal activities and the places of cash delivery and remittance by the counterparty in a cash transaction; (4) the places of sending, receiving, and arrival of instant messaging-based information or advertising and promotional information used for criminal activities; (5) the places of sale, network access, and concealment of a Modem Pool, a GOIP, a SIM box, or any other hardware used for criminal activities; and (6) the places of sale and login of an Internet account used for criminal activities.[313]

---

[312] See. Article 5 of the *Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of Telecommunications Network Fraud and other Criminal Cases* [最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见].

[313] See. Article 1 of the *Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of*

At the same time, in 2021, the Supreme People's Court made concluding provisions on the criminal jurisdiction of cybercrime in its judicial interpretation on the application of the 2018 revised Criminal Procedure Law： For a crime committed against or by mainly using a computer network, the place of a crime shall include without limitation (1) the place of the server employed by the network service used to commit the crime, (2) the place of the network service provider, (3) the place of the harmed information network system and its administrator, (4) the place of the information network system used by the defendant or victim in the course of crime, (5) the place of the victim at the time of sustaining harm, or (6) the place where the victim sustains a property loss.[314] It is worth mentioning that this provision does not deliberately distinguish between the above-mentioned places involved which are the places of criminal acts and which are the places of the result of the crimes.

To sum up, China's current regulations on the place of cybercrime go beyond the original binary structure (criminal acts and criminal consequences) and turn to a new direction. Specific to the jurisdiction of cybercrime cases, it means that the location of any element involved in cybercrime could be the place where the cybercrime was committed. Furthermore, the court of the place where the cybercrime was committed has jurisdiction over the first instance of that cybercrime case.

5. REGIONAL INTERNATIONAL COOPERATION AND CHINA'S CHOICE

This chapter has discussed China's legal system, cyber policies, cyber laws, and cybercriminal law in the preceding sections. They are all legal means against cybercrime at the domestic level. This section will focus on China's legal means of governing cyberspace, maintaining information security, and combating cybercrime at the international level.

Because of the globalization of the Internet, all the countries arguably share the same cyberspace. No single country could isolate itself from the Internet, so do China though there is a notorious firewall in the process of Internet access. Therefore, cyberspace governance or combatting cybercrime is a common issue that should be faced and tackled by the whole world with every country's effort. However, there is currently no universal international treaty to deal with cybercrime at the United Nation level. In the current world, it seems that

---

Telecommunications Network Fraud and other Criminal Cases (II) [最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）].

[314] See, Article 2 of the *Interpretation of the Supreme People's Court on the Application of the Criminal Procedure Law of the People's Republic of China (2021)* [最高人民法院关于适用《中华人民共和国刑事诉讼法》的解释(2021)]

nearly all of the treaties, agreements, or conventions that focus on cybercrime are regional international to some extent, such as the Budapest Convention on Cybercrime, the Arab Convention on Combating Information Technology Offences, and the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security. Though many countries signed, they do not cover all the countries worldwide and are just regional international agreements. At present, a comprehensive international convention for countering cybercrime and promoting international cooperation of cyberspace governance at the UN level has not been formulated. Regional international cooperation still plays a vital role in securing local cybersecurity and combatting cybercrime. Therefore, at least until the first UN-level convention on cybercrime is adopted, the primary path to achieving global governance of cybercrime should be to gradually improve common understanding of cybercrime, to maintain cybersecurity, and to build consensus for achieving universalization and globalization, all while fully recognizing the role of regional international cooperation in cyberspace.

The international cooperation on governing cyberspace, securing cybersecurity, and combatting cybercrime in China is mainly in the regional international form as most countries elsewhere. China's choice is basically constructed under the framework of information network security cooperation of the Shanghai Cooperation Organization (SCO). This section will focus on SCO's cooperation on cybersecurity, and the role of China plays in it.

5.1 SCO AND ITS MEMBER STATES

Regional international integrations can be broadly classified into three categories in today's world. The first focuses on economic cooperation by establishing a free trade zone, a customs union, and a common market and economic union. The most representative is the North American Free Trade Agreement (NAFTA). The second focuses on political cooperation, similar to the SCO. The third type is comprehensive, focusing on a single geographic region and everything associated with it, including political and economic affairs, such as the European Union. One critical point to mention is that as the SCO's cooperation deepens, its focus is not solely on political cooperation but also on economics, security, and other national issues. Regional international integrations are increasingly becoming comprehensive rather than serving a single purpose.

Like all the regional international integrations, SCO is based on geographic locations at first. "The Shanghai Cooperation Organization (SCO) is a permanent intergovernmental

international organization, the creation of which was announced on 15 June 2001 in Shanghai (China) by the Republic of Kazakhstan, the People's Republic of China, the Kyrgyz Republic, the Russian Federation, the Republic of Tajikistan, and the Republic of Uzbekistan. The Shanghai Five mechanism preceded it." [315] All these six countries are located, or their territory is mainly located in the east and middle Asia, which are neighbor countries. As for regional international integration is the popular way to negotiate and cooperate with the same situational countries. These six countries treat the SCO as a better approach to keep independent in the regional governance, seek the optimal interest in the regional cooperation, and sustain an active international voice.

In 2017, the Republic of India and the Islamic Republic of Pakistan were granted full members of the SCO. Thus, there are eight countries with full membership in SCO. Meanwhile, the SCO has four observer states, namely the Islamic Republic of Afghanistan, the Republic of Belarus, the Islamic Republic of Iran, and the Republic of Mongolia; and six dialogue partners, namely the Republic of Azerbaijan, the Republic of Armenia, the Kingdom of Cambodia, the Federal Democratic Republic of Nepal, the Republic of Turkey, and the Democratic Socialist Republic of Sri Lanka. The SCO has become the most prominent regional international organization with a large population that occupies 44% of the world's population and the grandest territory area. [316]

"On the principles of mutual trust, mutual benefit, equality, mutual consultations, respect for cultural diversity, and a desire for common development, while its external policy is conducted per the principles of non-alignment, non-targeting any third country, and openness,"[317] the SCO endeavor to build a multiple and comprehensive cooperation in the regional affairs including but not limited to the nuclear weapons, terrorism, education, criminal justice, economics, hygiene. Information security and cybercrime are included as well.

5.2 SCO'S COOPERATION IN CYBER AFFAIRS AND CHINA'S ROLE

5.2.1 SCO's Cooperation in Governing Cyberspace

[315] SHANGHAI COOPERATION ORGANIZATION: *About SCO*. The SCO Secretariat, 19 March 2019, http://eng.sectsco.org/about_sco/

[316] SOHU FINANCE: *Shocked!!! The SCO has become the most populous and largest regional cooperative organization in the world* [震惊!!! 上合组织成为世界上人口最多、面积最大的地区合作组织了]. Sohu News, 20 March 2019, https://www.sohu.com/a/149073133_169746

[317] SHANGHAI COOPERATION ORGANIZATION: *About SCO*. The SCO Secretariat, 19 March 2019, http://eng.sectsco.org/about_sco/

The SCO member states agree that cyberspace should be effectively managed. In September 2013, the SCO issued the Bishkek Declaration, which stated that the member states are committed to building a peaceful, secure, fair and open information space based on the principles of respecting national sovereignty and non-interference in the internal affairs of other countries, opposing the use of information and communication technologies for undermining political, economic and social security of the member states, preventing the use of the Internet to propagate terrorist, separatist and extremist ideologies, and supporting the elaboration of the universal rules, principles and standards of states' responsible behavior in the information space.[318] The SCO issued the Qingdao Declaration in June 2018, stating that member states will continue to bolster cooperation in order to jointly address cyberspace's challenges. At the same time, member states believe that it is necessary to respect each country's cyber sovereignty, which allows for equal participation in the development and governance of the Internet.[319] On the occasion of its twentieth anniversary in September 2021, the SCO issued the Dushanbe Declaration, which reaffirmed the importance of enhancing cooperation among member states in cyberspace governance and respect for states' cyber sovereignty in managing the Internet.[320]

The SCO member states advocate for the establishment of international cyberspace norms within the United Nations framework. In September 2011, the four SCO member states jointly submitted an *International Code of Conduct on Information Security* to the 66th sessions of the United Nations General Assembly. The document proposed a voluntary set of rules that included strict enforcement of cyber sovereignty, which grants a government the legal authority to enforce its own laws within its own borders and to control data flow.[321] In January 2015, the six SCO member states resubmitted to the UN an updated *International Code of Conduct on Information Security* and called for the establishment of multilateral, transparent, and democratic international Internet governance mechanisms that ensure equitable resource distribution, facilitate access for all and ensure the Internet's stability and

[318] See. *Bishkek Declaration: By the Heads of the Member States of the Shanghai Cooperation Organization*. 13 September 2013, http://eng.sectsco.org/documents/

[319] See. *Qingdao Declaration of the Council of Heads of State of the Members of the Shanghai Cooperation Organization* [Циндаоская декларация Совета глав государств членов Шанхайской организации сотрудничества]. 10 June 2018, http://eng.sectsco.org/documents/

[320] See. *Dushanbe Declaration of the Twentieth Anniversary of the SCO* [Душанбинская Декларация Двадцатилетия Шос]. 17 September 2021, http://eng.sectsco.org/documents/

[321] See. DE JONG-CHEN JING: Data Sovereignty, Cybersecurity, and Challenges for Globalization. *Georgetown Journal of International Affairs*, vol. 16. no. S1. (2015) 112-122.

security.[322]

5.2.2 SCO's Cooperation in Securing Cybersecurity

The SCO member states agree that their member states' cybersecurity is threatened by a variety of factors. In June 2006, the Shanghai Summit of the SCO States' Heads of State recognized that member states are facing military, criminal, and terrorist threats in the field of cybersecurity and that they must take immediate action to address the challenges collaboratively. The SCO places cybersecurity threats on an equal footing with threats to weapons of mass destruction.[323] Simultaneously, the member states of the SCO established an international expert group on information security. The Group of Experts has two permanent bodies within the SCO: the Secretariat and the Executive Committee of Regional Anti-Terrorist Structure of SCO (SCO RATS).[324]

In October 2015, the SCO member states held a cyber counter-terrorism maneuver code-named "Xiamen-2015" in Xiamen, China. This is the SCO's first coordinated cyberterrorism maneuver. Through the maneuver, member states exchanged their competent authorities' work processes, legal procedures, organizational and technical capabilities for combating cybercrime and the use of the Internet for terrorist purposes. On the other hand, it strengthened the mechanism for cooperation between member states' relevant organs in detecting and preventing the use of the Internet for terrorist purposes. Simultaneously, an initial technical platform for online counter-terrorism has been established.[325] In June 2017, the SCO signed the *Conventions of the Shanghai Cooperation Organization on Combating Extremism* in Nur-Sultan. According to the Convention, member states can maintain cybersecurity by monitoring the media and the Internet and promptly detecting and blocking the spread of extremist ideas; restricting access to extremist material on the Internet, and holding information network service providers criminally liable for non-compliance with

[322] See. *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?* CCDCOE: The NATO Cooperative Cyber Defence Centre of Excellence, 24 March 2022, https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/

[323] See. *Statement by the Heads of Member States of the Shanghai Cooperation Organization on International Information Security*. 15 June 2006, http://eng.sectsco.org/documents/

[324] See. SCO RATS: *About SCO RATS: History*, Regional Anti-terrorist Structure of Shanghai Cooperation Organisation, 24 March 2022, https://ecrats.org/en/history/

[325] See. *First Maneuver of Cyber Anti-Terrorism in Shanghai Cooperation Organization* [上合组织首次演练网络反恐], Xinhua News Agency, 2 May 2019, http://www.xinhuanet.com//politics/2015-10/15/c_128318903.htm

orders requiring restrictions on access to extremist material.[326] In November 2020, SCO further emphasized the necessity for member states to strengthen the fight against the use of the Internet to spread terrorist ideologies in order to safeguard cybersecurity.[327]

Simultaneously, China and Russia collaborate actively in the field of cybersecurity through the SCO. In May 2015, the foreign ministers of China and Russia signed the *Agreement on Cooperation in the Field of International Information Security between the Governments of the People's Republic of China and the Russian Federation*.[328] The agreement is divided into ten chapters. The agreement identifies the fundamental threats to international cybersecurity and establishes the fundamental direction, principles, forms, and mechanisms for China and Russia's cooperation in the field of international cybersecurity. At the same time, the Agreement views the use of ICTs to undermine internationally recognized norms, such as interfering in other States' internal affairs, undermining the sovereignty and political and economic stability, and inciting hostility between peoples or sects, as significant threats to the field of international cybersecurity.

5.2.3 SCO's Cooperation in Combatting Cybercrime

The SCO's cooperation in combating cybercrime is primarily manifested through the development of an agreement. At the Yekaterinburg Summit in June 2009, the SCO member states signed the *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization* (hereinafter referred to as the SCO Agreement). The agreement is the SCO's first regional international agreement to address cybersecurity and cybercrime in a systematic manner. The SCO agreement is quite

---

[326] See. *Conventions of the Shanghai Cooperation Organization on Combating Extremism* [Конвенции Шанхайской организации сотрудничества по противодействию экстремизму] [上海合作组织反极端主义公约], 9 June 2017, https://docs.cntd.ru/document/542655220?marker=64U0IK / http://www.npc.gov.cn/npc/c30834/201812/2cf58e34ebfa46ea8bd64a44c2cb6f9f.shtml

[327] See. *Statement by the Council of Heads of State of the Shanghai Cooperation Organization on countering the spread of terrorist, separatist and extremist ideologies, including on the Internet* [Заявление Совета глав государств-членов Шанхайской организации сотрудничества о противодействии распространению террористической, сепаратистской и экстремистской идеологии, в том числе в сети Интернет]. 10 November 2020, http://eng.sectsco.org/documents/

[328] See. [中华人民共和国政府和俄罗斯联邦政府关于在保障国际信息安全领域合作协定] [Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности], 8 May 2015, http://treaty.mfa.gov.cn/Treaty/web/detail1.jsp?objid=1531877059881 http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1

succinct. It is divided into 12 articles and two annexes.[329]

Article 1 and Annex I of the SCO Agreement define the agreement's basic terms. Articles II and Annex II detail the primary threats to cybersecurity, including cybercrime, that SCO member states face. Article III outlines the SCO Agreement's primary areas of cooperation, including the formulation of necessary common measures, the establishment of a threat monitoring and joint response system, the improvement of international standards, the fight against cyberterrorism and cybercrime, and the enhancement of legislative communications. Article IV defines the basic principles of cooperation within the framework of the SCO Agreement, including principles that contribute to social and economic development, principles of maintaining international stability and security, and principles of compliance with international law; and emphasizes respect for member states' cyber sovereignty and respect for principles of human rights and fundamental freedoms. Article V details the SCO Agreement's primary modalities and mechanisms of cooperation. The exchange of information and consultations will take place semi-annually in the SCO Secretariat or on the territory of invited member states, with the competent organs of member states responsible for the SCO Agreement's implementation serving as the primary body. Article VI of the SCO Agreement protects information used in cooperation. Under the premise of respecting member states' national interests, member states are permitted to withhold information involving state secrets during the course of cooperation. Article VII regulates the costs associated with the SCO Agreement's implementation. Article VIII establishes the SCO Agreement's relationship with other international treaties. Article 9 provides for the resolution of disputes arising during the interpretation and application of the SCO Agreement through consultation and negotiation. According to Article X, the SCO Agreement's working languages are Russian and Chinese. Article XI states unequivocally that the SCO Secretariat is the SCO Agreements' depositary. Article XII regulates the SCO Agreement's procedural matters such as the entry into force, amendment, accession, and withdrawal.

5.3 Comments and Discussions

The SCO Agreement adopts a legislative structure of "main text + annex" for the concept of terminology and provisions acknowledging the major cybersecurity threats confronting member states. This approach is unique from the basic connotations of

[329] See. *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization*. 16 June 2009, http://eng.sectsco.org/documents/

cybersecurity or cybercrime in other regional international agreements, which are defined in the main text rather than the appendix. Adopting this legislative model would contribute to the agreement's flexibility and updating while preserving the agreement's integrity. Member States may amend and supplement the text in light of actual developments and changes in circumstances through consultations in the annex rather than the main text. However, such an approach would result in a more general and vague agreement's content. For example, in Annex I of the SCO Agreement, *cybercrime* is defined as "using information resources and/or influencing them in the information space for illegal purposes." According to China's criminal law provisions, not all unauthorized use of information resources should be classified as a crime and punished under the criminal law. For instance, China's cybercrime provisions generally require severe circumstances. There could be no uniform definition or connotation of cybercrime within member states (at least in China). Thus, the definition in Annex I to the SCO Agreement may be a purely symbolic piece of legislation with no significant or practical implications, as a further interpretation of specific acts is required.

While SCO member states are increasingly aware of cybercrime's transnational and cross-regional characteristics, the SCO Agreement does not include provisions for criminal justice assistance in combating cybercrime. Cooperation in the joint fight against crime is based on the *Agreement on Cooperation in Combating Crime between the Governments of the Member States of the Shanghai Cooperation Organization*. The agreement was signed in Tashkent in June 2010. The agreement expressly provides that: "This Agreement does not affect the matters of legal assistance in criminal cases and extradition. The Parties shall cooperate on these issues according to the international treaties they are parties to and taking into account the Parties' legislation."[330] This means that SCO member states must make use of other bilateral or multilateral criminal justice assistance treaties in order to combat transnational cybercrime. Additionally, the absence of necessary criminal justice assistance provisions has resulted in a lack of enforcement of the SCO agreements in combating cybercrime to some extent.

Additionally, the SCO's cooperation on cyber matters is largely limited to the declarations of its annual summit of heads of state and the documents of various conferences. By and large, there are more forms than substances. For instance, the SCO Agreement's legislation is far too broad to adequately reflect the uniqueness of local needs. It reduces the

[330] See. *Agreement on Cooperation in Combating Crime between the Governments of the Member States of the Shanghai Cooperation Organization*. 11 June 2010, http://eng.sectsco.org/documents/

SCO agreement to a declaration rather than a comprehensive international agreement with substantive rights and obligations; cyber counterterrorism maneuvers have taken place only once and are still in their infancy. As a result, some Chinese scholars believe that the SCO's agreements on cyber cooperation have not been implemented in their entirety. It has harmed the SCO's development.[331]

However, although the SCO has some problems in cooperation in cyber affairs, it is, after all, a regional international organization in which China is mainly a member. It demonstrates that China, through cooperation with regional international organizations, is committed to cyberspace governance, cybersecurity, and cybercrime prevention.

This dissertation argues that the best way to address cyberspace governance, cybersecurity, and cybercrime is through the establishment of international agreements at the United Nations. However, the reality is that establishing a unified and accepted-by-all global standard for governing cyberspace, ensuring cybersecurity, and combating cybercrime is exceedingly difficult (at least, as far as the current situation is concerned, it does not exist). As a result, it is critical to overcome prejudice, seek the greatest possible convergence of interests among all countries, and strengthen and improve substantive cooperation in governing cyberspace, protecting cybersecurity, and combating cybercrime within the existing framework of regional international organizations.

[331] See. e.g., WENWEI ZHANG: Information Security Cooperation under Shanghai Cooperation Organization: Necessity, Current Situation, and Prospect [上海合作组织信息安全合作：必要性、现状及前景]. *Russian, East European & Central Asian Studies* [俄罗斯东欧中亚研究], vol. 3. no. 5. (2016) 94-106.

IV. EVALUATIONS AND REFLECTIONS OF CHINA'S PRACTICE ON CYBERCRIME: THE CONVICTION PRACTICE

On the Analysis of Policies and Legal Dogmatics of Current Legislation

The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for Internet governance's future. Two independent global think tanks, the Centre for International Governance Innovation and Chatham House, established it to conduct and support independent research on the Internet-related dimensions of global public policy for the future of Internet governance.[332]

The GCIG pointed out four fundamental issues which need to be paid more attention to in cyberspace governance, namely, ensuring human rights online (focusing on the protection of privacy and free expression), enhancing legality of cyberspace governance (as well as in dealing with cybercrime), stimulating economic innovation and growth (including policies of encouraging technological innovation of new economic forms), and avoiding systemic risk (including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues). [333]

Based on fully considering and drawing on the four basic issues that need attention in cyberspace governance proposed by the GCIG, this chapter will focus on the manifestations and existing problems of the first three issues in China's cyberspace and cybercrime governance. This chapter selects three aspects as the conviction practice of China's cybercrime governance to echo the fundamental considerations raised by the GCIG.

The first section of this chapter will discuss China's full implementation of the Internet Real-name system to illustrate the issue of ensuring human rights online within China's context. This section also echoes China's cyber policy discussed in Chapter III. Some scholars believe that the Internet real-name system is a product of China's implementation of the cyber sovereignty policy to defend China from terrorism, pornography and Western values.[334] However, the question of whether the online real-name system will be

[332] CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION (CIGI): *Global Commission on Internet Governance (2014–2016): About the GCIG*, 25 March 2022, https://www.cigionline.org/activities/global-commission-internet-governance-2014-2016/

[333] See. LESLIE DAIGLE: *On the Nature of the Internet*. Centre for International Governance Innovation and Chatham House, 13 March 2022, https://www.cigionline.org/static/documents/gcig_paper_no7.pdf

[334] See. TOM HOLT, JOSHUA D. FREILICH, STEVEN CHERMAK AND CLARK MCCAULEY: Political

effective in achieving cybercrime prevention in China and whether it will restrict the right to privacy and free expression will be the focus of this section.

The second section of this chapter will discuss China's crackdown on online obscene live broadcasting to illustrate the current state of China's efforts to strengthen the legality of cybercrime governance. As introduced in Chapter II, cyber-porn and obscenity fall into the category of cybercrime. Pornography, also known as obscenity, is the representation of sexual situations and content for the purpose of sexual arousal and stimulation.[335] It is available online in a variety of formats.[336] The Internet and computer-mediated communications enable individuals to identify, publish, consume, and distribute sexual materials of all kinds to anyone, regardless of age, sexual orientation, or preference.[337] They facilitate the economy of paid sexual services which may not be legal in a given area, such as China.[338] Online obscene live broadcasting, supported by viewers who pay the broadcasters for their obscene show, is a new form of cyber-porn and obscenity of cybercrime.[339] The focus of this section is on China's conviction practice of this new form of cybercrime under current criminal law.

The third section of this chapter will discuss how to strike a balance between China's cybercrime governance and the promotion of the Internet sharing economy through technological innovation, using DIDI's ride-hailing business as an example under Article 286(I) of the Criminal Law of the People's Republic of China. The third section will examine whether DIDI can be punished for the large number of criminal cases that have occurred on its platform, based on the *Crime of Refusing to Fulfill the Obligation of Information Network Security Administration* (a morphology of cybercrime in China, see Chapter II-2.2); and discuss current Chinese practices.

Radicalization on the Internet: Extremist Content, Government Control, and the Power of Victim and Jihad Videos. *Dynamics of Asymmetric Conflict*, vol. 8. no. 2. (2015) 107-120.

[335] See. FREDERICK LANE: *Obscene Profits: Entrepreneurs of Pornography in the Cyber Age*. New York, Routledge, 2001.

[336] See. SUSAN W. BRENNER: Defining Cybercrime: A Review of Federal and State Law. In: RALPH D. CLIFFORD (ed): *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*. Raleigh, Carolina Academic Press, 2011. 15-104.

[337] See. JAMES F. QUINN AND CRAIG J. FORSYTH: Red Light Districts on Blue Screens: A Typology for Understanding the Evolution of Deviant Communities on the Internet. *Deviant Behavior*, vol. 34. no. 7. (2013) 579-585.

[338] See. THOMAS J. HOLT AND ADAM M. BOSSLER: *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. London and New York, Routledge, 2016.

[339] See. JOSHUA W. ROBERTS AND SCOTT A. HUNT: Social Control in a Sexually Deviant Cybercommunity: A Cappers' Code of Conduct. *Deviant Behavior*, vol. 33. no. 10. (2012) 757-773.

1. Dynamic Balance between Cybercrime Prevention and Human Rights Protection: Reflections on the Internet Real-name System in China

For disposing of cybercrime, most countries in the world applied different measures to deal with cybercrime, including legislation and agreements of both the national and international levels. Amongst the practice of all countries, there is one policy, which focuses on the anonymity of the Internet, called Internet Real-name System or Network Real-name Registration System.

Internet Real-name system is not a new policy in the world. It was first applied at the official level in South Korea in 2002 and abolished by the Korean Constitution Court.[340] It could be said that failure is the first Internet Real-name System at the national level. However, in China, by the promulgation of the Cybersecurity Law, the Internet Real-name System is fully applied now. At the same time, on 21 September 2018, Legal Daily published an article that some scholars and official staffs in China keep revisiting this system to make it more efficacy. Their womb view is to insist on using this system but needs some improvements.[341] Some criminal law scholars also believe that beneficial is the Internet Real-name System to prevent cybercrime, especially in the Situation Crime Prevention paradigm.[342]

This section will first introduce the Internet Real-name System, including what the Internet Real-name System is and the typologies. Second, this section will restrict the scope in China, not the world level, and enumerate the legal documents which are effective in China now and give some comments on them. Third, this section will provide a brief look at crime prevention from a criminology perspective, then redefine cybercrime prevention and find the correspondence to the crime prevention theories. Fourth, this part will rationally analyze the relationship between cybercrime prevention and the Internet Real-name system. Limitations on human rights, especially privacy and free expression, will also be briefly discussed in the Chinese context.

---

[340] KEECHANG KIM: Korean Internet and Real Name Verification Requirement. *Korea University Law Review*, vol. 20. (2016) 87-104.

[341] XIAO DU AND ZIXUAN FU: *Legal Rules and Technical Rules Need to Blend With Each Other* [法律规则与技术规则需彼此交融]. Legal Daily, 11 December 2018, http://legal.people.com.cn/n1/2018/0921/c42510-30306323.html

[342] DAOCUI SUN: Coordinated development between criminal governance and Network Register System [网络实名制与刑事治理的协同化思考]. *Journal of Nanjing University of Post and Telecommunication (Volume of Social Science)* [南京邮电大学学报（社会科学版）], vol. 18. no. 3. (2013) 16-24.

1.1 INTERNET REAL-NAME SYSTEM: DEFINITION AND CATEGORY

1.1.1 Definition: Refine the concept of Internet Real-name System

When discussing the Internet Real-name System, it is necessary to first discuss its concept. There are many different names of the Internet Real-name System, such as the Network Registration System[343], Real-name Verification System[344], Internet Censorship System[345], Real-name Policy[346], etc. All these names can be seen as a kind of description or generalizations of the Internet Real-name System. So, when we do the information retrieval in the database, we should consider the different expressions of the Internet Real-name System.

However, a closer examination of these names reveals that requirements for clients' true identity when using ICT are critical. In other words, the Internet Real-name System's central requirement is that Internet users link their real identities to the ones they use on the Internet or in Cyberspace.

The people's real identity consists of accurate personal information or data that contains the real name, gender, telephone number, ID number, working place, living address, and so forth. By these data or information, the government or the Internet companies can unveil a person's anonymity online[347], and the user can be precisely recognized and located when some subjects need to find out an individual account's owner online. As a result, the Internet Real-name System's core requirement is to establish a one-to-one correspondence between real and virtual identities.

To sum up, the Internet Real-name System should be such a system, which requires network participants to link factual personal information with virtual identities in the

---

[343] JYH-AN LEE AND CHING-YI LIU: Real-Name Registration Rules and the Fading Digital Anonymity in China. *Washington International Law Journal*, vol. 25. no. 1. (2016) 1-34.

[344] JOHN LEITNER: Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals. *Journal of Korean Law*, vol. 9. no. 1. (2009) 83-108.

[345] JEFFREY LI: Internet Control or Internet Censorship: Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice. *Pittsburgh Journal of Technology Law and Policy*, vol. 14. no. 1. (2013) 1-[i].

[346] See. SANDRA SCHMITZ: Facebook's Real Name Policy: Bye-Bye, Max Mustermann? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC)*, vol. 4. no. 3. (2013) 190-204; MARGOT KAMINSKI: Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech Articles. *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 23. no. 3. (2012) 815-896.

[347] DANIEL J. SOLOVE: Digital Dossiers and the Dissipation of Fourth Amendment Privacy. *Southern California Law Review*, vol. 75. no. 5. (2002) 1083-1168.

registration or online services acceptance stage of cyber-activity in the cyberspace, through a mandatory or voluntary way, to achieve the effect of the so-called Real-name system. It should be known that it is compulsory in China now.

1.1.2 Category: Types of Internet Real-name System in practice

The various classification criteria reflect the Internet Real-name System's multiple focuses. It is an appropriate approach for developing a holistic view of the system. The Internet Real-name System can be classified into two types based on the different subjects that require users to perform real-name verification.

The Governmental Internet Real-name System is based on formal normative documents, such as laws, acts, regulations, and policies. In general, the Governmental Internet Real-name is compulsory. All Internet participants should obey these regulations.

The other one is the Corporate Internet Real-name System or the Vocational Internet Real-name System, based on industry standards and user agreements. The Corporate Internet Real-name is voluntary at the user's level but mandatory at the company's level. In other words, the users can decide whether to accept the requirement of the real-name policy. If they are dissatisfied with one company's policy, they have the option of switching to another or discontinuing the use of related Internet applications. But the company should follow its industry standard.

The Internet Real-name System could also be classified into three types based on the various stages of Internet participation.

The first is the Real-name in Accessing the Internet. It means the user should do the real-name verification or check-in when they try to access the Internet, for example, buy the SIM card, check-out the broadband network, and so on. In many countries, this is mandatory. For instance, in Japan, mobile phones and SIM cards are bound to sell. The user should use the ID card or driver's license to register on the SIM card.[348]

The second is the Real-name in Providing Internet Service. It overlaps the Real-name in Accessing the Internet with its specialty. It refers to the Internet service provider, mainly when providing online services after accessing the Internet. In practice, its subject is primarily the Internet corporates but also some e-commerce partners. For example, retailers online, when someone wants to sell something online on the Amazon or Taobao website, they

[348] See. YUEJIANG WEI: How Countries Around the World Implement Internet Real-Name System [世界各国如何推行网络实名制]. *Shanghai Informatization* [上海信息化], no. 3. (2013) 82-86.

have to register with a real identity.[349]

The third type is Real-name in Accepting the Internet Service. It requires the users to supply real identity when they are accepting the online service. For example, if a person wants to register an email address, he must offer real identity to complete the registration process. Furthermore, depending on the different types of online services, some mainstream online services require the users to provide real identities in China, such as real-name in online games, real-name in online trading, real-name in online social media, or social communications, and so forth.

1.2 RELATED MEASURES IN CHINA: LEGISLATIONS AND COMMENT

1.2.1 Normative on Internet Real-name System

Generally, implementing an Internet Real-name System was not accomplished in one action in China. The foundation of the legal system as to Internet Real-name System endured a long process from 2000. Some scholars hold the view that the Internet Real-name System emanated from 2002.[350] This section agrees with the first point, 2000. In 2000, the State Council of China promulgated one administrative regulation named *Regulation on Internet Information Service* [互联网信息服务管理办法]. It had been revised in 2011. In the revised one, all Internet service providers have been divided into profitable and non-profitable.[351] "The State establishes a licensing system for profitable Internet information service and a filing system for non-profitable Internet information service."[352] It means whatever profitable or non-profitable providers are. They should submit their real identity to the administrative authorities if they want to provide Internet service.[353] As talked about above, this is the Real-

[349] See. Article 24 of the *Measures for the Supervision and Administration of Online Trading* [网络交易监督管理办法]: An online trading platform operator shall require a business that applies for selling commodities or providing services on the platform to submit true information on its identity, address, contact information, and administrative licensing, among others, conduct verification and registration, establish registration archives, and verify and update relevant information once at least every six months [网络交易平台经营者应当要求申请进入平台销售商品或者提供服务的经营者提交其身份、地址、联系方式、行政许可等真实信息，进行核验、登记，建立登记档案，并至少每六个月核验更新一次].

[350] See. YIFEI GAO AND LIAN JIANG: The Development and Regulation on the Internet Real-name System [网络实名制的发展及其规制]. *Social Science in Guangxi* [广西社会科学], no. 2. (2016) 102-108.

[351] See. Article 3 of the *Administrative Measures for Internet Information Services* [互联网信息服务管理办法]: Internet information service is divided into two categories: profitable Internet information service and non-profitable Internet information service [互联网信息服务分为经营性和非经营性两类].

[352] See. Article 4 of the *Administrative Measures for Internet Information Services* [互联网信息服务管理办法]

[353] See. Article 8 of the *Administrative Measures for Internet Information Services* [互联网信息服务管理办法]: A non-profitable Internet information service provider shall file for record its activities at telecommunications administrative authorities of the provinces, autonomous regions and cities under the

name in providing Internet Service.

In 2002, to strengthen the administration of business sites of Internet access services, the State Council of China promulgated the *Regulations on the Administration of Business Premises of Internet Access Service* [互联网上网服务营业场所管理条例]. It had been revised three times separately in 2011, 2016, and 2019. This regulatory document requires the user to use the real identity in the business sites of Internet access services.[354]

In 2005, according to the requirements of the bureau of public security of Shenzhen in Guangdong Province of China, Tencent Co. launched the real-name registration to the founders and administrators of the QQ group chat.[355] This work seemed like significant progress, marking the beginning of the full implementation of the Internet Real-name System in China.[356] The State Council Information Office and Ministry of Post and Telecommunications (reorganized in 2008 to Ministry of Industry and Information Technology) passed two regulatory documents governing the IP address and Internet news information service in the same year. There are some articles as to real-name requirements in these two regulatory documents.[357]

With the development of online trading, China's government pays more attention than it first appeared. In 2009 and 2014, the Ministry of Commerce and the State Administration

---

direct control of the Central Government or the Ministry of Information Technology (MII), and the following documents shall be submitted: (1) basic information of the service provider and its person-in-charge; […] [从事非经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门办理备案手续。办理备案时，应当提交下列材料:(一)主办单位和网站负责人的基本情况；[…]].

[354] See. Article 23 of the *Regulations on the Administration of Business Premises of Internet Access Service* [互联网上网服务营业场所管理条例]: An operating entity shall verify and register the identification cards or other valid certificates of the Internet users, and shall record the relevant net information. The registration and records reserved shall be kept for at least 60 days, and shall be provided when the departments of culture administration or public security consult them pursuant to law. The registration and records reserved may not be modified or deleted during the period of keeping [互联网上网服务营业场所经营单位应当对上网消费者的身份证等有效证件进行核对、登记，并记录有关上网信息。登记内容和记录备份保存时间不得少于 60 日，并在文化行政部门、公安机关依法查询时予以提供。登记内容和记录备份在保存期内不得修改或者删除].

[355] "Tencent Co. is the largest Internet company that offers online instant communication services and online games with the largest numbers of customers in China. QQ is one of its products." See. SALLY FRENCH: *China has 9 of the world's 20 biggest tech companies*. Market Watch, 13 December 2018, https://www.marketwatch.com/story/china-has-9-of-the-worlds-20-biggest-tech-companies-2018-05-31

[356] YIFEI GAO AND LIAN JIANG, 2016, p. 103.

[357] *Provisions for the Administration of Internet News Information Services* [互联网新闻信息服务管理规定] (It has been revised in 2017 by the Cyberspace Administration of China); *Measures for the Administration of IP Address Archiving* [互联网 IP 地址备案管理办法].

for Industry and Commerce (reorganized in 2018 to State Administration for Market Regulation) have formulated two normative documents for the administration and guidance of the online business.[358] The Real-name requirement is easy to find in these two documents, especially for online retailers.

In 2010, considering the impact of online games on minors, the Ministry of Culture (reorganized in 2018 to Ministry of Culture and Tourism) promulgated departmental rules to regulate the chaos of online games in China. As discussed above, it requires the customers of online games to offer real identity to judge a user, whether the major or minor. It is a kind of real-name requirement in the area of online games' administration. [359]

In 2012, the Standing Committee of the National People's Congress promulgated a piece of decisions to build the fundamental principles of the real-name policy.[360] After that, the Ministry of Industry and Information Technology ordered users to link real identities with a telephone in 2013[361] and short communication messages in 2015[362].

Till 2016, all the regulatory documents on the requirements of the real-name system were scattered and without a particular law. Then, in 2016, China promulgated the Cybersecurity Law to build the Internet Real-name System of Internet service providers from an overall perspective.[363]

---

[358] *Online Shopping Service Standards of 2009* [网络购物服务规范]; *Administrative Measures for Online Trading of 2014*［网络交易管理办法］(It had been expired since the enactment of the *Measures for the Supervision and Administration of Online Trading* [网络交易监督管理办法] in March 2021.)

[359] See. Article 16 of the *Interim Measures for the Administration of Online Games* [网络游戏管理暂行办法] (It had been revised once in 2017 and repealed in 2019.)

[360] See. Article VI of the *Decision of the Standing Committee of the National People's Congress on Strengthening Information Protection on Networks* [全国人民代表大会常务委员会关于加强网络信息保护的决定]: Network service providers which provide the website access service for users, handle landline or mobile phone network access procedures for users or provide the information publishing service for users shall, when signing agreements with users or confirming the provision of services, require users to provide their true identity information [网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息].

[361] See. *Provisions on the Registration of True Identity Information of Telephone Subscribers* [电话用户真实身份信息登记规定].

[362] See. *Provisions on the Administration of Communications Short Message Services* [通信短信息服务管理规定].

[363] See. Article 24 of the *Cybersecurity Law of the People's Republic of China* [中华人民共和国网络安全法]: Where network operators provide network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information release services, instant messaging services and other services, they shall require users to provide true identity information when signing agreements with users or confirming the provision of services. If any user fails to provide his

1.2.2 Impartial Comments of China's strategy

Regarding the above-mentioned introduction of regulatory documents for the Internet Real-name System in China, we can observe several characteristics.

The Internet Real-name System starts relatively early in China. Though some scholars recognize that it starts from 2002, as discussed above, it starts from 2000. The continuous application of the Internet Real-name System is a process of constant improvement and comprehensiveness in China. The foci of the Internet Real-name System changes from the Internet Service Provider to the Internet Service Provider and the User together. Real-name in Accessing the Internet is not the only emphasis, but also the Real-name in Providing the online service and Real-name in Accepting the online service.

Because China has already constructed a relatively entire legal system on the real-name system, including the laws, regulations, departmental rules, and departmental regulatory documents, the Internet Real-name System is the Governmental Internet Real-name System, which means this requirement or policy is dominant by the government. In other words, it is compulsory and direct in the whole state cyberspace in China. It is very different from the Vocational Real-name System, which is based on vocational standards. Most of the countries with the Internet real-name system applied this kind of requirement: users are mandatory to provide personal information such as name, address, Email, and so forth personal data to the network operators when buying a mobile phone or applying for accessing the Internet, and then, by the clerk, the customer's name, address, ID number, and other personal information would enter the database of the operators, indirectly in the form of real-name registration to implement network real-name system. This indirect real-name registration mainly concentrates on European and American countries that pay much attention to protecting freedom of speech. In addition to adopting indirect real-name methods, these countries also impose strict restrictions on the scope of real-name networks. For example, in the United States, only a few fields or websites such as 'Facebook' and 'Google+' require a real name.[364] However, in recent years, the scope of the network real-name system in the United States has expanded.[365]

---

or her true identify information, the network operator shall not provide him or her with relevant services [网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务].

[364] See. YUEJIANG WEI, 2013, p. 86.

[365] See. YIFEI GAO AND LIAN JIANG, 2016, p. 106.

Though the directness of the Internet Real-name requirement is the prominent feature in China's strategies, it is improper to look upon the Internet Real-name System in China as the direct type rather than the indirect one. Indeed, China offers an elective plan that 'real names in the background and either real names or screen names in the foreground under free wills.'[366] (thereinafter 'Mandatory in Background, Voluntary in Foreground') It means the user should provide real identity when they register for Internet service. The operator should back up this information. However, the users can use the online service with a pseudonym on the screen.

1.3 CRIME PREVENTION AND CYBERCRIME PREVENTION

To determine whether the Internet Real-name System facilitates cybercrime prevention in practice (or not), it is necessary to grasp two key concepts: the Internet Real-name System, which we discussed in the preceding two subsections; and cybercrime prevention. If we are to have a firm grasp on cybercrime prevention, we must first understand crime prevention. If we are to have a firm grasp on cybercrime prevention, we must first understand crime prevention.

1.3.1 Crime Prevention: Implications, Framework, and Typologies

Crime prevention is a criminological notion. It locates in the responding to the crime in criminology and occupies a distinct position to the other responding to the crime. Crime prevention takes preventive approaches, which are proactive and based on the assumption that crime can be predicted to some extent and therefore avoided by taking precautionary steps in advance to minimize the incidence of committing crimes or eradicate the occurrence of crimes.[367] Its premise is that with the accurate methods effectively applied, relevant expertise, and sufficient resources, we can understand the motivation of human behaviors and the causes of crimes, then the crime can be precisely anticipated. In turn, appropriate interventions can be taken to eradicate the crime or substantially reduce the frequency of

[366] See. Article 6 of the *Interim Provisions on the Administration of the Development of Public Information Services Provided through Instant Messaging Tools* [即时通信工具公众信息服务发展管理暂行规定]: Service providers of instant messaging tools shall, under the principle of "real names in the background and either real names or screen names in the foreground under free wills," require service users of instant messaging tools to register accounts upon authentication of their real identity information [即时通信工具服务提供者应当按照"后台实名、前台自愿"的原则，要求即时通信工具服务使用者通过真实身份信息认证后注册账号].

[367] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS: *Criminology*. New York, Oxford University Press, 2017, p. 600.

crime.[368]

On the face of it, crime prevention should aim to prevent crime, but its aim is relatively complex in practice. Crime prevention should at least focus on three areas: "(a) criminogenic (risky situations); (b) potential offenders (risky people); and (c) vulnerable groups or communities ('at risk' people)."[369]

Notably, people feel anxious about some crimes that do not happen to them. For example, there is a high incidence of violent crimes in a certain region. Although violent crimes do not persecute some groups, they still worry about this situation. Therefore, crime prevention should reduce the incidence of crime and take some measures to reduce people's anxieties.

As a result, crime prevention objectives should include: "(a) divert potential offenders from crime; (b) avoid 'bad lives'; (c) safeguard potential victims; (d) provide reassurance to the general public; (e) promote community safety; (f) protect commercial interests; (g) build social capital, and (h) defend the moral order."[370]

Numerous scholars have advanced numerous theoretical models and practical measures in order to accomplish the goal of crime prevention. For example, Brantingham and Faust proposed a framework for policy and practice based on primary, secondary, and tertiary prevention ideas. [371] Primary preventions concentrate on modifying and managing the criminogenic conditions or risky situations both in the physical and social environment.[372] The secondary preventions devote themselves to identifying and intervening to reduce the likelihood of individuals or groups on the way to offend. The tertiary preventions focus on systematically decreasing the possibility of further offending or recidivism. "The primary preventions offered the most propitious prospects, and this, therefore, prompted a significant shift in an effort towards the wider-ranging environment and social programs."

Regarding the identification in the secondary prevention, Crawford believed that we

---

[368] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017, p. 601.

[369] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017, p. 602.

[370] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017, p. 608.

[371] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017, p. 606.

[372] PAUL J. BRANTINGHAM AND FREDERIC L. FAUST: A Conceptual Model of Crime Prevention. *Crime & Delinquency*, vol. 22. no. 3. (1976) 284-296.

could not reasonably identify who would offend, where, and when because of the limited technologies, knowledge, and the changing circumstance.[373] In addition to this suspicion, the authors of the framework also considered whether it would be helpful to establish a framework covering all interventions within the purview of the criminal justice system. As we consider the whole framework, we can find out that all the functions that existed in this framework are sometimes beyond the remit of the criminal justice system; and, which is visible and, in fact, has been proved that crime prevention needs more collaboration with methods out of the criminal justice system.

Then here comes the three main types of crime prevention models or measures: community, developmental, and situational crime prevention. Community crime prevention is looked upon as a combination of developmental and situational prevention to some extent.[374] Furthermore, community crime prevention initiatives are difficult to conclude precisely regarding their efficacy or "the methods by which beneficial outcomes are achieved."[375] So, we mainly discuss developmental crime prevention and situational crime prevention in this part.

Developmental crime prevention is founded on the presupposition that: "Traits or propensities conducive to antisocial conduct and crime develop in the womb and early in childhood. The roots of crime thus extend over the life course." [376] Following this presupposition, if we want to pre-empt the commission of crimes, we need continuous and developmental interventions to reduce crime inducement factors and provide alternative social opportunities in the early years and at later stages in one's life.[377]

Situational crime prevention is based on opportunity theories,[378] composed of the Rational Choice Perspective, the Routine Activity Approach, and the Crime Pattern

[373] See. ADAM CRAWFORD: *Crime Prevention and Community Safety*. London, Longman, 1998.

[374] BRANDON C. WELSH AND DAVID P. FARRINGTON: Crime Prevention and Public Policy. In: BRANDON C. WELSH AND DAVID P. FARRINGTON (eds): *The Oxford Handbook of Crime Prevention*. Oxford, Oxford University Press, 2012. 3-22.

[375] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017, p. 616.

[376] FRANCIS T. CULLEN, MICHAEL L. BENSON AND MATTHEW D. MAKARIOS: Developmental and Life-Course Theories of Offending. In: BRANDON C. WELSH AND DAVID P. FARRINGTON (eds): *The Oxford Handbook of Crime Prevention*. Oxford, Oxford University Press, 2012. 23-45.

[377] FRANCIS T. CULLEN, MICHAEL L. BENSON AND MATTHEW D. MAKARIOS, 2012, p. 26.

[378] See. RONALD V. CLARKE AND KATE BOWERS: Seven Misconceptions of Situational Crime Prevention. In: NIKE TILLEY AND AIDEN SIDEBOTTOM (eds): *Handbook of Crime Prevention and Community Safety*. New York, Routledge, 2017. 109-142.

Theory.[379] This model and these three theories will be thoroughly discussed in the next section with cybercrime prevention.

1.3.2 Cybercrime Prevention: Redefinition and Correspondence

Cybercrime is a series of harmful deviant behaviors taken for procuring improper interests forbidden by law or common social values, by the feature of the data and online transportation thereof, which abuse the advanced technologies and the information asymmetries that get from positional advantages.

In the light of the definition of crime prevention above, we could redefine cybercrime prevention in the form of through a range of preventive initiatives to reduce the incidence of cybercrime gradually, thereby eradicating the cybercrime, meanwhile, by the preventative measures, to promote cybersecurity and improve the protection of the personal information. The ultimate objective of cybercrime prevention is to make cyberspace a better and safer environment for improving and developing technology, lifestyle, and well-being of human society. In line with the features of cybercrime, cybercrime prevention exhibits some of the characteristics corresponding to that.

From the perspective of appearance, the overall impression of cybercrime prevention reflects a strong dependence on technology. People use firewalls to prevent Trojans from intruding and use new encryption algorithms to protect personal information. Every week, anti-virus software on our computers updates the computer virus database to deal with unknown risks. Mobile payment procedures have also begun to use a combination of biometric information and traditional passwords to secure transactions. The applications of these technique initiatives reflect the method of crime prevention introduced by Crawford that "increases the required effort to commit the crime."[380]

From the characteristics of Internet development, the globalization of the Internet makes cybercrime prevention require global cooperation. No country can completely isolate the Internet. Criminals may have committed cybercrime against country B in country A. So, as Tilley said that "Crime, in general, is complex, with many features, causes, motivations, and conditions […] it will not be possible for any agency on its success to address all aspects

[379] See. MARTHA J. SMITH AND RONALD V. CLARKE: Situational Crime Prevention: Classifying Techniques Using "Good Enough" Theory. In: BRANDON C. WELSH AND DAVID P. FARRINGTON (eds): *The Oxford Handbook of Crime Prevention*. Oxford, Oxford University Press, 2012. 291-315.

[380] See. ADAM CRAWFORD AND KAREN EVANS: Crime Prevention and Community Safety. In: ALISON LIEBLING, SHADD MARUNA AND LESLEY MCARA (eds): *The Oxford Handbook of Criminology*. Oxford, Oxford University Press, 2017. 797-824.

of all crime prevention problems."[381] Transnational cooperation in cybercrime prevention requires a relatively uniform system of crime prevention that is acceptable to all parties. However, it is challenging to establish a unified, replicable, and transferable cybercrime prevention system. Although many attempts have been made, such as the SCO Agreement, the effect is not apparent as discussed in Chapter III-5.4.

In addition, cybercrime prevention is an evolving and continuously updated system of crime prevention. Though this feature is inherent in crime prevention, cybercrime prevention presents more prominent instability.

First, from the usual Internet behavior to justify the criminalization of change, such as hacking was not originally cybercrime and as the behavior of heroism, but the subsequent abuse led to its criminalization.[382]

Second, the behavior in the physical space is projected into cyberspace to produce corresponding more severe crimes. For example, bullying behavior evolves into cyberbullying in cyberspace, and due to the immediacy and extensiveness of Internet transmission, the impact of cyberbullying far exceeds the damage in physical space.

Third, cyberspace itself derived a new type of crime, the frequency of such updated criminal offenses far beyond the physical space. The types of crime in the traditional physical territory are relatively stable and fixed, but the development of cybercrime makes the cybercrime group more active.

Based on the above-mentioned inexhaustible enumeration characteristics, the cybercrime prevention system needs to adjust policies continually and change strategies regularly to cope with new risks of offending. A logical connotation here is that traditional crime prevention measures endorsed by the previous theories are not well adapted to the new requirements. It presents the instability of cybercrime prevention systems.

1.4 Dialectical Relationship: Internet Real-name System and Cybercrime Prevention

1.4.1 Logical Starting Point: Eradicate Anonymity

[381] NICK TILLEY: Crime Prevention in Britain, 1975-2010: Breaking Out, Breaking In, and Breaking Down. In: GORDON HUGHES, EUGENE MCLAUGHLIN AND JOHN MUNCIE (eds): *Crime Prevention and Community Safety: New Directions*. London, Sage, 2002. 12-36.

[382] See. SUSAN W. BRENNER: *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Boston, Northeast University Press, 2012. pp. 15-28.

Anonymity can provide a "shield from the tyranny of the majority"[383] or "a mask used to protect the perpetrator of a crime."[384] There are four types of anonymity: (a) traceable anonymity, (b) untraceable anonymity, (c) traceable pseudonymity, and (d) untraceable pseudonymity.[385]

The untraceable anonymity means the user does not identify himself and is not identifiable ultimately. It is rather challenging to realize in the physical world because of the development of forensic technologies. However, it is easy to achieve in cyberspace, and here, many governments approve and justify the regulation thereof.[386] Governments are afraid of perfect crimes caused by complete untraceable anonymity.[387] Most users in cyberspace are of traceable anonymity "through intermediaries or other identifiers."[388] It is the kind of Internet Real-name System that most countries apply. The users should submit their personal accurate identity information to the intermediary or registry of some sort, and these institutions will keep the information in their database. As long as not using the anonymizing software, even most anonymous users are traceable by the upcoming switch to IPv6.[389]

Pseudonymity is different from anonymity. It adopts a developing and ongoing identity that can develop an image and reputation by itself.[390] "By contrast, anonymity is sometimes attained through passivity, rather than through active speech."[391] Pseudonymity allows for a shared voice or identity when adopted by many users at one time. For example, the online account name can be the same as many people. Like anonymity, pseudonymity can be categorized into two types, as mentioned above. Untraceable pseudonymity is that the user identifies himself by a pseudonym and cannot be identified ultimately. Traceable pseudonymity allows others to trace the identity of the user behind the pseudonym.[392] From a policy perspective, traceable and untraceable pseudonymity and anonymity cannot be distinguished measurably. So, in this part, the term anonymity includes pseudonymity.

---

[383] See. *McIntyre v. Ohio*, 514 U.S. 334, 357 (1995).

[384] MARGOT KAMINSK, 2012. p. 817.

[385] A. MICHAEL FROOMKIN: Legal Issues in Anonymity and Pseudonymity. *Information Society*, vol. 15. no. 2. (1999) 113-127.

[386] A. MICHAEL FROOMKIN: Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases. *Journal of Law and Commerce*, vol. 15. no. 2. (1995) 395-508.

[387] A. MICHAEL FROOMKIN: Lessons Learned Too Well: Anonymity in a Time of Surveillance. *Arizona Law Review*, vol. 59. no. 1. (2017) 95-160.

[388] MARGOT KAMINSK, 2012. p. 821.

[389] MARGOT KAMINSK, 2012. p. 822.

[390] MARGOT KAMINSK, 2012. p. 822.

[391] MARGOT KAMINSK, 2012. p. 823.

[392] A. MICHAEL FROOMKIN, 1999, p. 113-127.

It is generally believed that the anonymity of the Internet leads to the occurrence of cybercrimes. Although there is no precise research data to support the correlation, people still maintain stereotypes. As with the discussion of cybercrime prevention, people prefer to consider anonymity as a critical factor therein. By eradicating the anonymity in cyberspace and re-designing cyberspace's environment, cybercrime could be prevented to some extent. This aspect is inherent in the pursuit of the Internet Real-name System; on the other hand, consistent with the theoretical model of situational crime prevention.

According to the rational choice perspective, decisions as to whether to offend are based on a deliberate calculation on the potential offender's part of the "risks, rewards and efforts of alternative courses of action."[393] The offenders or the potential ones will consider the time, ability, and knowledge about the circumstance, and if the calculation suggests that the reality is to their advantage, they will commit crimes. The Internet Real-name System requires all the participants to provide real identity to reduce anonymity. It improves the risk of being caught when the offenders finish committing a crime. For this, the offenders need more effort or knowledge to conceal their identity online. So, the cost of engaging in cybercrime will weigh the rewards thereof. Then, cybercrime prevention can attain.

According to the routine activity approach, it considers the coincidence of three factors: "a motivated offender, a suitable target for the offenses, and the absence of a capable guardian to prevent the crime from occurring."[394] If these three factors in routine activities of various parties to the crime converge at a particular time and place, then the coincidence will be more likely to occur. Turning to the Internet Real-name System, eradicating anonymity is equivalent to building arguably useful preventive guardians. That is to say, if a potential offender wants to commit cybercrime, he must first take a range of measures to overcome the obstacles of transparent identity brought by eradicating anonymity. To a certain extent, this can prevent potential offenders who cannot break through the guardian from committing cybercrime and thus achieve the goal of cybercrime prevention.

To sum up, by reducing anonymity in cyberspace, the Internet Real-name System enables a methodical approach to reducing opportunity, creating inhibitors, and creating uncertainty on the outcomes of cybercrime. In China, the Internet Real-name System eliminates anonymity to implement situational crime prevention of cybercrime. Thus, one

[393] MARTHA J. SMITH AND RONALD V. CLARKE, 2012, p. 294.

[394] MARTHA J. SMITH AND RONALD V. CLARKE, 2012, p. 296; STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017, p. 618.

could conclude that the Internet Real-name System's starting point is the abolition of anonymity.

1.4.2 External Experiences: A Korean Case

China is not the only country that applied Internet Real-name systems around the world. Indeed, as we mentioned above, many countries have used the Internet Real-name System to some extent.[395] South Korea had applied the Internet Real-name System at the official and national levels. Prior to 2016, when China established the Internet Real-name System, South Korea was the only country on Earth to do so through legislation. It was a mandatory requirement for all Internet participants.

In 2000, Korean society showed the highest Internet subscription rate in the world.[396] Many Internet subscribers and easy access to the Internet in Korea lead to the speedy exchange of information and equally rapid formation of public opinions. [397] Such advantages with the Internet amplify the injuries of the defamation and intervention of privacy.

In 2004, the real-name requirement first appeared in the Election of Public Officers Act.[398] It was introduced for preventing the "illegal election campaigning activities on the Internet such as the circulation of false rumors and libels about candidates."[399] Therefore, at first, the real-name requirement existed in the area of political kinds of stuff. However, because of the case "Dog feces woman" or "Dog poop woman,"[400] Korean society began to

---

[395] See. YUEJIANG WEI, 2013. pp. 82-86.

[396] K. S. PARK: Mandatory Identity Verification in the Internet: Did Google Do the Right Thing. *Korea University Law Review*, vol. 5. (2009) 203-224.

[397] K. S. PARK, 2009, p. 203.

[398] Article 82-6(1): Where an Internet Media Company offers the facility for users to post opinions about an election in its bulletin board, chart room etc., the Internet Media Company shall implement technical measures so as to allow the posting only when the name and the resident's registration number supplied by the user intending to post the opinion correspond to the person's real name and the resident registration number.

[399] K. S. PARK, 2009, p. 205.

[400] See. YU SONG: *[World Vision] The Rise and Fall of South Korean Network Real-Name System* [天下远见：韩国网络实名制兴废记]. infzm.com. 24 December 2018, http://www.infzm.com/contents/67455 [The "Dog poop woman" was the nickname of the case which a woman did not clean up the feces from her pet dog on the subway in South Korea in 2005. The woman was recorded and photographed by one Internet user, and then these pictures were submitted to the Internet. Many anonymous left a great number of verbal malignant words to abuse the woman. Some Internet users also found her real name, work place, and home address, and shared these pieces of information with other Internet users. The woman and her family had to apologize to the public. Their lives were harassed by the Internet users rigorously. Then, the woman had suffered from serious mental illness in the end. The perpetrator became the victim. This incident prompted the Korean society to reflect the cyber violence.]

show great concern for the regulations on the Internet for personal use in daily life. Then, the Korean government is en route to making a far more comprehensive act to regulate all online actions. In 2007, Korea promulgated the amendment of the *Act to Promote the Use of Information and Communication Network and to Protect Information* [정보통신망 이용촉진 및 정보보호 등에 관한 법률] (thereinafter ICNA). [401] Article 44-5(1) of this act demand all the private websites with a certain number of users every day and all the public entities websites to apply measures of some sort to verify the users' real identity, regardless of the content of the user's postings.[402] At this point, it can be said that South Korea has fully established the Internet Real-name system. However, the bill had not been implemented for several years, and its introduction had been fraught with controversy.

Its original intention is to resist cyber libel. But, an empirical study of the Internet Real-name system in Korea showed a decrease in the rate of malign online posts from 15.8% to 13.9%.[403] "This is not necessarily inconsistent with other research[404], which showed a small decrease in defamatory replies."[405] In 2012, the South Korean Constitutional Court ruled that the Internet real-name system established under ICNA should be abolished due to the following:

> *"To restrict freedom of expression in advance, it is necessary to demonstrate the effect on the public interest clearly. […] The number of illegal postings did not decline significantly after the Internet real-name system was implemented; rather, users fled to foreign sites. Given the occurrence of reverse discrimination, it is difficult to assert that the public interest is being served. […] Given that it restricts freedom of expression, makes it more difficult for foreigners without a resident registration number to use the Internet bulletin board, and increases the possibility of information leakage to the outside, the disadvantage cannot be said to outweigh the public interest. […] Thus, the ICNA's provisions establishing the identity verification system violate the principle of excessive prohibition and infringe on the claimant's fundamental rights, including freedom of expression, self-determination of personal*

[401] KEECHANG KIM, 2016, p. 92.

[402] KEECHANG KIM, 2016, p. 92.

[403] JOHN LEITNER, 2009, pp. 97-98.

[404] JEONG MIN CHOI, HYUN SOO NA AND JI SUK WOO: An Empirical Analysis of the Effect of the Real-Name System on Internet Bulletin Boards: How the Real-Name System and User Characteristics Influence the Use of Slanderous Comments and Swear Words. *Korean Journal of Public Administration*, vol. 48. no. 1. (2010) 71-96. (In this paper, it shows the decrease from 13.9% to 12.2%.)

[405] JOHN LEITNER, 2009, pp. 97-98.

information, and freedom of the press."[406]

1.4.3 Evaluation: Functions Realization and Value Balance

The preceding subsection described how South Korea declared the Internet real-name system unconstitutional. The reasoning process of the judges of Korea's Constitutional Court is highly regarded as a model. The South Korean Constitutional Court's logic is clear. Suppose the Internet real-name system can achieve its function well to produce significantly more public benefits than its reduced public interests. In that case, the Internet real-name system is not unconstitutional. Otherwise, it is a violation of the Constitution.

Now, shift your focus to China. According to situational crime prevention theory, China's initial goal in developing and implementing the Internet real-name system was to prevent cybercrime. Then, following the logic of the South Korean Constitutional Court, as long as China's Internet real-name system effectively prevents crime and reduces the rate of cybercrime, it can be considered a good system. On the other hand, if China's Internet real-name system fails to effectively prevent crime and introduces numerous disadvantages, it is unreasonable. Thus, two questions must be addressed in order to determine the reasonableness of China's Internet real-name system. The first is whether it has done an adequate job of preventing cybercrime. The other is whether the sacrifices brought by its implementation are less than the benefits of its implementation. This section encapsulates these two issues as functional realization and value balance.

1.4.3.1 Functional Realization

Internet real-name system as a preventive approach for preventing cybercrime would have some connatural limitations in itself thereby restricting the realization of the function of the prevention.[407] These limitations or consequences are an escalation, displacement, adaption, deflection, and injuries amplification of the cybercrime.[408]

First are the escalation and displacement of cybercrime under the implementation of the Internet Real-name system. Grabosky suggested that "the construction of physical barriers

---

[406] See. *The Constitutional Court of South Korea ruled that the Internet real-name system violated the Constitution* [헌재 "인터넷 실명제 위헌" (종합)]. Yonhap News Agency, 23 August 2012, https://www.yna.co.kr/view/AKR20120823156200004

[407] See. DAOCUI SUN, 2013, pp. 16-18.

[408] PETER N. GRABOSKY: Unintended Consequences of Crime Prevention. In: ROSS HOMEL (ed): *The Politics and Practice of Situational Crime Prevention*. New York, Criminal Justice Press, 1996. pp. 25-56. (A typology of regressive outcomes of crime prevention includes crime escalation, displacement, overdeterrence, and perverse incentives.)

may invite their defacing or destruction. The frustration that results from blocked criminal opportunity may lead to expressive violence, or to an instrumental reliance on more forceful means of goal attainment."[409] The Internet Real-name system deters potential offenders from committing a cybercrime by the risk of detecting and investigating efficiently. Then the offenders would turn the traditional cybercrime, such as cyber-fraud, cyber-libel, and so on, to the crime targeting the data or information backed up in the ISP's database, which is easy to get through without efficient techniques to improve the index of safety in some small ISPs. As the appendage of accurate identity authentication, personal data is of stimulus for the potential offenders. On the other hand, the difficulty of committing the relative traditional cybercrime and the appearance of a new criminogenic objective would result in the intensive occurrence of identity theft and misuse. Thus, the Internet Real-name system is provocative rather than preventive.

Second is cybercriminals' adaptation and cybercrime deflection. The Internet in China is different from the one in other countries, except North Korea. Rather than the Internet, it is better to say China is using the most prominent local area network in the world by the state-enforced firewall be of block external information, especially the information from Google's related products. Moreover, under the circumstance of the full implementation of the Internet Real-name System, the offenders have to conceal their identities and locations when they intend to commit a cybercrime. In general, they will both use a fake identity and VPN services of some sort to achieve the goal.

Furthermore, the deflection of cybercrime will happen. Cybercrime will transmit from the surface web to the deep web or dark web to use particular software. The cyber-police should locate and trace the IP address for a more effective cybercrime investigating. Here is the paradox: without the Internet Real-name system, the most helpful method to investigate cybercrime is locating the IP address; even with real-name authentication, it is still an effective way to deal with the deflection of cybercrime. Then the Internet real-name system will become formalism and only increase the cost of ISPs managing the data they get from users. In addition, China's Criminal Code criminalizes the conduct of a large amount of data breaching the ISP for management's negligence. It would also add the risk of violating the criminal law for ISPs. To sum, the Internet Real-name system as a preventive measure for cybercrime prevention neither very effectively realizes cybercrime prevention nor decreases the burden on ISPs.

[409] PETER N. GRABOSKY, 1996, p. 27.

The last is the amplification of injuries of cybercrime. According to the rational choice theory, the offender would consider the cost and the profits and find the best balance before committing a crime. For those who have determined to commit cybercrime, the Internet Real-name system increases their cost without a doubt for committing whereby the exploiting of particular software to conceal some crucial information. Then the offenders would try to get more profits from the crime, which at the same time causes more loss of victims. Or, from another angle, cybercrime has become more severe than before. It is not exclusively the case, but cyber libel would be more harmful under the Internet Real-name system. Since China fully implements the Internet real-name system, almost all social media accounts are associated with a specific real-name identity. Although the real-name identities of the associated accounts may not be the users' real identities, at least in the eyes of other users, these accounts represent a true person in real life. Because people on the Internet prong to believe what comes from an actual person, some malign (essentially defamatory) statements are easily accepted. Then the victim would suffer more misery from the cyber libel.

1.4.3.2 Value Balance

In its preamble, the Universal Declaration of Human Rights emphasizes that States Members of the United Nations should take effective measures to universally and effectively recognize and observe it.[410] Article 12 of the Universal Declaration of Human Rights provides for the right to privacy and reputation.[411] Article 19 of the Universal Declaration of Human Rights provides for the right to freedom of opinion and expression.[412] As a member of the United Nations, China shall recognize and observe the provisions of the Universal Declaration of Human Rights. In fact, the above-mentioned rights to privacy and freedom of expression have been written into China's constitution. Article 33 of the *Constitution of the*

[410] See. The preamble of the *Universal Declaration of Human Rights*: [P]roclaims this Universal Declaration of Human Rights as a common standard of achievement for all peoples and all nations, to the end that every individual and every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the peoples of Member States themselves and among the peoples of territories under their jurisdiction.

[411] Article 12 of the *Universal Declaration of Human Rights*: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[412] Article 19 of the *Universal Declaration of Human Rights*: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

People's Republic of China stipulates that: "The state respects and protects human rights." Article 35 stipulates that: "Citizens of the People's Republic of China enjoy the *freedom of speech, of the press*, of assembly, of association, of the procession and of demonstration." Article 40 stipulates that: "Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon citizens' freedom and privacy of correspondence, except in cases where, to meet the needs of state security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law."

One could argue that the Chinese Constitution and the United Nations Declaration of Human Rights are generally consistent. As a United Nations member, this demonstrates that China has taken a sincere intention to implement the Universal Declaration of Human Rights. On the other hand, it demonstrates the universality of human rights. In other words, the universality of fundamental human rights is beyond question.[413] Their connotations should be consistent, and there should be no variation in the connotations of rights due to country-specific differences.

So, does China's full implementation of the online real-name system infringe on the above human rights?

First, as far as the right to free expression is concerned, the Internet real-name system attempts to eliminate the anonymity online in China entirely. However, no matter the anonymity is a kind of expression or just a kind of conduct in the speech[414], it is the core factor under the freedom of expression. There is no doubt about this. Many cases in the United States[415] have already manifested that, though restriction is placed on the right of

---

[413] See. *Vienna Declaration and Programme of Action (1993)*. A/CONF.157/23, Geneva: UN, 12 July 1993.

[414] MARGOT KAMINSK, 2012, pp. 846-847. ("Some courts treat mask-enabled anonymity as conduct rather than speech; some look to the content of the masks to determine if the mask-wearing is expressive; others observe that anonymity is inherently entwined with expression and freedom of association")

[415] See. e.g. *NAACP v. Alabama*, 357 U.S. 499 (1958) ("Compel disclosure of one's identity may dissuade persons from exercising their freedom of speech for the fear of reprisals."); *Talley v. California*, 362 U.S. 60 (1960) ("The anti-mask statute would tend to restrict freedom to distribute information and thereby freedom of expression.); Cohen v. California, 403 U.S. 15 (1971) ("Specific means of communication is protected because the speaker's choice of medium itself is often expressive."); *Buckley v. Valeo*, 424 U.S. 1 (1976) ("The anti-mask statute would tend to restrict freedom to distribute information and thereby freedom of expression."); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) ("The anti-mask statute would tend to restrict freedom to distribute information and thereby freedom of expression."); *Virginia v. Black*, 538 U.S. 343 (2003) ("A state may permissibly regulate 'statements where the speaker means to communicate a

anonymity, it is still essential in exercising the First Amendment right, Freedom of Expression.[416] The decision of the Constitutional Court of South Korea also confirms that the internet real-name system is a pre-set measure to restrict freedom of expression. South Korea's experience showed that after the implementation of the Internet real-name system, the number of posts on main web pages had decreased significantly. The Internet Real-name system in China, which hinged on accurate identity verification and exacting scrutiny, would arguably be tantamount to suppression of, or infringement of, the freedom of expression. Prohibiting anonymity online would chill the unpopular or controversial speech online ineluctably. Forbidding anonymity would reduce the "total of information and opinion contributed to the public debate." [417]

Second, as far as the right to privacy is concerned, the official staff of the Ministry of Public Security of China gave some comments on implementing the Internet Real-name system from the overall establishment in 2016 to 2018.[418] Li Jingjing, director of the Legal Affairs Office of the Cyber Security Bureau of the Ministry of Public Security, held the view that the real-name verification, which is based on the Cybersecurity Law, requires the Internet Service Provider to verify the real identity of the users, and these measures inevitably lead to the providers keep the user's information in their database. It will increase the risk of information breaching, and in fact, it is a severe problem in Chinese society nowadays. By the national strategies of 'Internet +,' more and more traditional industries have started to connect to the Internet. Personal information, a form of big data, has become an area with business chances and commercial profits. A large amount of personal information in the ISP database through real-name authentication has become an unprotected fat sheep. A variety of interest groups, including criminal groups, are eyeing this fat. It will lead to more people committing new cybercrime targeting personal information. At the same time, whether it is a long-term or short-term use of the Internet, Internet user registration constitutes a very

---

serious expression of intent to commit an act of unlawful violence to a particular individual or group of individuals'.") (*Virginia v. Black* presumably narrows the scope of the anonymity, but still protects it.)

[416] See. *Aryan v. Mackey*, 462 F. Supp. 90 (N.D. Tex. 1978); *Ghafari v. Municipal Court for San Francisco Judicial District of San Francisco*, 87 Cal. App. 3d 255 (Cal. Ct. App. 1978). Retrieved from MARGOT KAMINSK, 2012, pp. 851-876. (These two cases introduced "anonymity not as a First Amendment right in itself, but as essential to the exercise of First Amendment rights under *NACCP v. Alabama*.")

[417] MARTIN H. REDISH: *The Adversary First Amendment: Free Expression and the Foundations of American Democracy*. Stanford, Stanford University Press, 2013, p. 161.

[418] XIAO DU AND ZIXUAN FU: *Legal Rules and Technical Rules Need to Blend With Each Other* [法律规则与技术规则需彼此交融]. Legal Daily, 11 December 2018, http://legal.people.com.cn/n1/2018/0921/c42510-30306323.html

important privacy concern. Identification of users has become an essential process when accessing the Internet. Either way, the identification mechanism of Internet users is a restriction on the right to privacy and anonymity.[419]

In addition, China's Internet Real-name system itself has certain logical loopholes. It only focuses on whether the user can provide a real personal identity and associate it with an account in cyberspace. In other words, if a person registers an account with the accurate identity information of others, it can also successfully pass the real-name review. This case is not alone, but there is a lot of reality. For example, minors will search online and use the identity information of other adults to pass the registration review of online games and adult websites. It is not a difficult thing to get a piece of accurate identity information online in China.

In summary, this section believes that China's Internet real-name system is unreasonable.

The first is because it does not achieve the original intent of the policy on the prevention of cybercrime. After China fully implemented the Internet real-name system, China's cybercrime has not been effectively curbed. On the contrary, the rate of cybercrime is rising year by year and is becoming the main form of crime in China.[420] Furthermore, the Internet Real-name system prevents cybercrime by challenging the right to free speech and privacy, as some scholars argued in their research.[421] The fundamental logic behind utilizing the Internet real-name system to achieve cybercrime prevention is to protect users from cybercrime by sacrificing some of their basic human rights. For instance, to protect females from rape or sexual harassment, they should wear a long dress that exposes less of their body. Women should avoid going outside in the evening, as some law enforcement personnel and

[419] TOBY MENDEL, ANDREW PUDDEPHATT, BEN WAGNER, DIXIE HAWTIN AND NATALIA TORRES: *Global Survey on Internet Privacy and Freedom of Expression*. Paris, United Nations Educational, Scientific and Cultural Organization (UNESCO), 2012, p. 33.

[420] "In terms of cybercrime cases, from 2016 to 2018, more than 48,000 cybercrime cases have been concluded. The number of cybercrime cases and its proportion occupied in all criminal cases have shown an upward trend year by year, and the number of cases in 2018 has increased significantly, up 50.91% year-on-year. In terms of cyber fraud cases, using the Internet to carry out fraud has become more and more serious. In 2017, cyber fraud cases accounted for only 7.67% of all fraud cases. However, its proportion soared to 17.61% in 2018. Nearly 20% of cyber fraud cases were scams carried out after obtaining citizens' personal information." See. *Press conference on 'Big Data Reports on Cybercrime' and 'Typical Cases of Cyber Fraud'* [网络犯罪大数据报告及电信网络诈骗犯罪典型案例新闻发布会], The Supreme People's Court of The People's Republic of China, 19 November 2019, https://www.court.gov.cn/zixun-xiangqing-200651.html

[421] See. e.g., JYH-AN LEE AND CHING-YI LIU, 2016, pp. 17-22; JOHN LEITNER, 2009, pp. 103-105; K. S. PARK, 2009, pp. 216-220; KEECHANG KIM, 2016, p. 103.

criminal justice scholars have recommended. These measures are *inadvisable* because they require victims to forego certain fundamental rights, such as freedom of dress and movement, to which they are entitled under the constitution or other regulations or culture, in order for the government to guarantee protection.[422] It can be verified well by a campaign called the "Reclaim the Night march," in which some women protest for equal protection at night in the United Kingdom.[423]

Second, it violates the human rights of citizens to a certain extent, including the right to privacy and freedom of expression. Numerous data breaches in China expose personal information to a significant risk of leakage and misuse. Statistics show that between 2010 and 2017, the crime of infringing on citizens' personal information showed a clear upward trend. They peaked in 2017 with a total of 1137 cases. Compared with 426 cases in 2016 (the year China passed the Cybersecurity Law and fully established the Internet real-name system), the number of cases in 2017 increased by 711.[424] At the same time, requiring citizens to participate in openGovernment under their real names resolves authentication issues for the government that uses the system, but results in users speaking less openly than they would if they spoke anonymously or pseudonymously.[425] This demonstrates how the requirement for an Internet real-name system does restrict citizens' freedom of expression.

The thorough implementation, without exceptions, of the comprehensive Internet Real-name system proscribed by China's Cybersecurity Law drew widespread criticism. The international academics treated China's approach to "block noncompliance and maintain the political power of the government"[426], thus failing to "build an ideal online environment with public order and trust."[427]

---

[422] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017, p. 612.

[423] See. RECLAIM THE NIGHT, 25 December 2018, http://www.reclaimthenight.co.uk/why.html. ("In every sphere of life, we negotiate the threat or reality of rape, sexual assault and sexual harassment. We cannot claim equal citizenship while this threat restricts our lives as it does. We demand the right to use public space without fear. We demand this right as civil liberty; we demand this as a human right.")

[424] See. *"Crimes of Infringing on Citizens' Personal Information" Special Case and Data Analysis Report* [《侵犯公民个人信息罪》专题案例与数据分析报告]. PKULAW.COM, 12 April 2018, http://weekly.pkulaw.cn/Admin/Content/Static/9a9869ed-5f02-446c-8637-ae8adbe3b308.html

[425] See. TOBY MENDEL, ANDREW PUDDEPHATT, BEN WAGNER, DIXIE HAWTIN AND NATALIA TORRES, 2012, pp. 38-39.

[426] K. S. PARK, 2009, p. 215. ("In case of China, the introduction of Internet Real-name system seems to actually have the form of censorship as a means to block information and maintain the political power of the current government regardless of inducement of healthy Internet culture or prevention of damage.")

[427] JYH-AN LEE AND CHING-YI LIU, 2016, p. 24. ("The effective enforcement of the [Internet Real-name

Although the Internet real-name system is ineffective at preventing cybercrime, despite the fact that it violates citizens' privacy and freedom of expression, and despite the fact that the Internet real-name system has failed in South Korea, the Chinese government still views the Internet's real-name system as a reasonable method of preventing cybercrime and will continue to use it in the future. China will not declare the Internet real-name system unconstitutional, as South Korea had done, but would strengthen it through additional legislation or regulations. This section argues that it would be imprudent to forego a constitutionally protected and internationally recognized fundamental human right in order to fulfill the cybercrime prevention function (that is, to fully implement the real-name system on the Internet in China without exception). Chinese citizens and governments should consider the relationship between the Internet real-name system's abandonment of anonymity and the human rights protected by international law and the Chinese Constitution, including the right to privacy and freedom of expression, and strike a balance in the governance of cybercrime.

1.5 STAGED SUMMARY

The establishment of the Internet Real-name system in China experienced progress from 2000 to 2018. As a mandatory Governmental Internet Real-name system, it has been expected to function cybercrime prevention as a part of cybercrime governance. Though failure was Korea's experience, China still insists on implementing this system. However, discussions in this section have already evidenced the implementation of the real-name requirement in China, accompanied by deviations and restrictions in exercising freedom of expression and personal privacy. Without considering the inherent limitations of the preventive measures of crime prevention, it is hard to say China has found the best balance between human rights protection and the demands on cybercrime prevention in cybercrime governance. Therefore, the motivation and purpose of full implementation of Internet Real-name system without any exceptions in China are doubtful and questionable.

Lessons should be learned from China's practice: Cybercrime governance at the expense of human rights protection can neither effectively govern cybercrime nor fully protect human rights. The formulation and implementation of cybercrime governance policies must be fully considered and discussed. On the one hand, scholars cannot simply agree to please the rulers. On the other hand, citizens should also keep a clear head and not be swayed by rampant propaganda about the threat of cybercrime, nor make concessions to their

System] may ironically run counter to China's original policy goal: to build an ideal online environment characterized by public order and trust.")

fundamental human rights. Properly grasping the dynamic balance between cybercrime governance policies and human rights protection is the real long-term solution to cybercrime governance.

2. The Principle of Legality in Criminal Law and Explanation Extension of Current Legislation on Cybercrime Governance: Reflections on Combatting Online Obscene Live-streaming in China

As Internet information technology evolves, so too do the modern lifestyles and forms of cybercrime. While dealing with, or coping with, the challenges of the new way of conventional crimes, different countries or international integrations would prefer the legislation as the primary and proactive strategy. Due to the hysteresis of law, previous law is often unable to respond quickly and effectively to new forms of crime. Here is the case that the different countries have to choose policies between enacting new regulations based on current statutes to achieve the result of controlling the new forms of crime and by way of legal or judicial, or both, interpretation or analysis of the legislative intent, of the existing ordinance to embrace the new forms of crimes into the criminal justice system in the present. In other words, *Explanation Extension of Current Legislation*.

On September 18, 2019, Finland, the presidency of the Council of the European Union, presented a revised 88-page proposal to the delegations on the Regulation on Privacy and Electronic Communications (Directive 2002/58/EC). It refers to the *Processing of electronic communications data for the purpose of detecting, deleting, and reporting material constituting child pornography.* Adult pornography might be legally protected within the realm of free speech in many countries[428], but child pornography is forbidden with culpability and responsibility worldwide.[429] All the states arguably criminalize online or offline child pornography. However, because of the broad and sweeping attitude against obscenity in China, both adult and child pornography are criminalized without any exceptions. Whether in legislation, law enforcement, or legal practice, China singled out pornography as the

[428] "In the U.S. and most Western nations, pornographic content is legal so long as the voluntary participants in the acts depicted and the consumer or viewer of the content are of the legal age for the country." See. THOMAS J. HOLT AND ADAM M. BOSSLER: *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. London and New York, Routledge, 2016, p. 13.

[429] "Law enforcement agencies around the world have invested substantial resources in the investigation and prosecution of child pornographers." See. THOMAS J. HOLT AND ADAM M. BOSSLER, 2016, p. 14.

predominant target of cybercrime to combat. Applying the filtering technology and approaches, building the Great Firewall of China, and aggravating the criminal penalty for pornography have been employed, the number of pornography web-users, however, increased year by year.[430] Recently, a new form of accessible media technology has made it easier to access online pornography and increasingly attracts more attention to online obscene live streaming.

Online live streaming is not a new technology in the world. Many media stations applied this for broadcasting the news, sports, and events. However, it turns to be out of control with the development of extensive use of the mobile terminal. Nowadays, building a platform for online live streaming by Apps in the App Store is convenient. Then the online lives could be different from the previous style by which traditional media companies controlled and escaped government supervision easily. Some criminals would utilize the above-mentioned features to make profits or get some other achievements by broadcasting or transiting illegal materials in online lives. Pornography is an example. Generally, if both the audience and hosts are adults in most other states, online obscene live streaming would not be illegal. This conduct might bear culpability or responsibility only when participators, either audience or hosts, are minors. Because it belongs to two different kinds of behaviors, one is child pornography, and the other is transiting pornography to minors. So, when some relative occurrences appeal to law enforcement or courts, the officials should first distinguish the different circumstances and then respond.

It is not the case in China cause all obscenity is forbidden. Furthermore, according to the unique context of China, a vast user base, and ban without exceptions, it is somewhat interactive to deal with or cope with this issue. As of the first half of 2019, the scale of online live streaming users in China has the potential to surpass 500 million. In addition, by application of the technology of 5G becoming gradually prevalent in China, the online live streaming industry is to keep stable development in the near future.[431] As for the statistics aforehand, there is no accurate calculation of the proportion of minors amongst the users. Nevertheless, we could hypothesize that the percentage of juveniles in online live streaming users could be arguably significant by the feature of cyberspace, which is more attractive to

[430] BIN LIANG AND HONG LU: Fighting the obscene, pornographic, and unhealthy--an analysis of the nature, extent, and regulation of China's online pornography within a global context. *Crime, Law and Social Change*, vol. 58. no. 2. (2012) 111-130.

[431] IIMEDIA RESEARCH CENTER: *2019 H1 China Online Living Streaming Market Research Report*. iiMedia Research Inc, 2019. 1-49.

young people,[432] and more than 70% of adolescents in China have their cell phones.[433] The Chinese government has already recognized this problem and employed a series of measures to eradicate online obscene live streaming. However, in practice, there are a lot of questions when responding to online obscene lives. There is a controversial debate amongst the legal practice that, on the one hand, contemporary law could not solve all the problems of online obscene lives, there is a strong demand for new legislation to tackle the issue, and before the new legislation, with the consideration of *The Principle of Legality in Criminal Law*, the whole society should tolerate this phenomenon; on the other hand, some scholars oppose that new technology updates the cybercrime every day, it could not solely rely upon the legislation but by way of an explanation extension of existed law to deal with the new problems, though the reality is the demand of new legislation. Here comes this section on balancing the actual needs for cybercrime governance with the persistence of *The Principle of Legality in Criminal Law*.

This section will first introduce the "CleanNet 2019" campaign in China, which aims to eradicate illegal materials online under Chinese law and penalize the criminals involved. At the same time, the following subsections will focus on some cases from the "CleanNet 2019" related to the online obscene live streaming. Secondly, this section will enumerate some debatable, but not all, difficulties and problems in the legal practices which encompass the application of criminal law, evidence law, and criminal procedure law. Thirdly, this section will discuss the questions before with comparative methods and *legal dogmatics*. In the end, this section will conclude all the discussions with a response to the preliminary question of this part, the balance between *The Principle of Legality in Criminal Law* and *Explanation Extension of Current Legislation*.

2.1 "CLEANNET 2019" CAMPAIGN AND REPRESENTATIVE CASES IN CHINA

2.1.1 SHDF National Office and "CleanNet 2019" Campaign

For dealing with the rampant social and criminal problems arising from pornography, prostitution, and illegal publication, the Chinese government had founded a working group specialized in controlling and governing the problems mentioned above by which named

[432] CATHERINE D. MARCUM, GEORGE E. HIGGINS AND MELISSA L. RICKETTS: Sexting Behaviors among Adolescents in Rural North Carolina: A Theoretical Examination of Low Self-Control and Deviant Peer Association. *International Journal of Cyber Criminology*, vol. 8. no. 2. (2014) 68-78.

[433] WEIMIN JI, JIE SHEN, BINYAN YANG AND LIN JI: *Annual report on the Internet use and reading practice of Chinese minors (2017-2018)* [中国未成年人互联网运用和阅读实践报告（2017～2018）]. Beijing, Social Science Academic Press (China), 2018.

national anti-pornography and illegal publication working group (扫黄打非工作组) in 2000. It consists of 26 official departments that contain the governmental departments and organs of the Communist Party of China. Its standing office, National Anti-pornography-and-illegal publication, usually called *Sao Huang Da Fei* National Office (hereinafter SHDF National Office) in Chinese, is affiliated to the Central Propaganda Department of the Communist Party of China.[434]

Since economic reform from the 1980s, Chinese society has experienced a great challenge of the ascending rates of crimes. Whether the administrative requirements or real social needs, they both demand the government to control the crimes effectively to ensure social harmony and safety. Under this rigorous political assignment, the Chinese government is used to pick up the severe strike campaign to deal with particular or general criminals involved in the target crimes. Though the effectiveness of the severe strike campaign as a crime control strategy has been questioned, the campaign-style crime control reserves the strong inertia effect in policy-making.[435] The Chinese government prefers the staged attack in the form of the campaign in every crime control, so too does the governance of pornography.[436] In this context, SHDF National Office employed the "CleanNet" campaign to suppress online obscenity in cyberspace. CleanNet campaign is one of the consisted actions applied by the SHDF National Office every year. It aims at recreating and rehabilitating the online environment by sweeping indecent materials that existed in web pages, cloud storage, instant communications, mobile applications, and so on. As routine actions, SHDF National Office deployed the "CleanNet" campaign again in 2019, referred to as "CleanNet 2019". According to the reported news on the website of SHDF National Office, "CleanNet 2019" will consist from April to November. Compared with the same theme campaign previously, "CleanNet 2019" has some unique features that aim at online pornography in the traditional area mentioned above and turn to the online live streaming platform. The SHDF National Office requires the legal enforcement agencies at different levels to keep supervising the unlawful online live streaming platform, relentlessly striking the criminals engaged in disseminating online indecent materials or organizing an online obscene live show, and resolutely shut down the relative software or mobile applications.[437]

---

[434] SHDF National Office: *About us*, 20 October 2019, http://www.shdf.gov.cn/shdf/contents/749/236131.html

[435] BIN LIANG: Severe strike campaign in transitional China. *Journal of Criminal Justice*, vol. 33. no. 4. (2005) 387-399.

[436] BIN LIANG AND HONG LU, 2012.

[437] SHDF NATIONAL OFFICE: *SHDF National Office deployed the "CleanNet 2019", "Nursing Seedling*

As of now, "CleanNet 2019" has been drawing to a close. There are some representative cases as the campaign's achievements reported to the SHDF National Office during the period. The next part will select some cross-sectional cases as to online obscene live streaming to introduce and discuss.

2.1.2 Representative Cases on online obscene live streaming in CleanNet 2019

As a result of ongoing within the "CleanNet 2019" campaign till now in China, the overall statistics of the case amount, criminals' situation, victims' distribution, and other information about this campaign could not elaborate. However, by way of the gradual implementation, the website of the SHDF National Office has reported some critical cases by which the local legal enforcement agency submitted and, therefore, as the achievements of their reasonable diligence in this campaign. This part selects five cases from the web page of the SHDF National Office that are typical to tailor-make the complicated circumstances of the contemporary realities of online obscene lives in China.

Guangxi Nanning Case.[438] In June 2019, Xi Xiang Tang District Court of Nanning city of Guangxi Province heard a case which prosecuted that *Li Mou Hua*, the perpetrator, arranged four persons to do online obscene live shows many times by online live streaming software during two days from July 18, 2018, to July 20, 2018. On July 20, 2018, the Xi Xiang Tang Bureau of Public Security found the clues of the online obscene live shows organized by *Li Mou Hua* when they were generally patrolling the cybersecurity situation in this district. Then, on July 24, 2018, the Xi Xiang Tang Bureau of Public Security detained the perpetrator. According to the litigation and evidence submitted by the prosecutors, the court sentenced *Li Mou Hua* to one-year imprisonment and a 2,000-yuan fine by citing Article 365[439] of the Criminal Law of the People's Republic of China (*Crime of Organizing Pornographic Performance* [组织淫秽表演罪]).[440]

2019" and "Autumn Wind 2019" Special Action [全国"扫黄打非"办公室部署开展"净网 2019""护苗 2019""秋风 2019"专项行动], 4 March 2019, http://www.shdf.gov.cn/shdf/contents/767/394202.html

[438] As multi-perpetrators involved in part of the selected five cases, this part would like to use the formula of "*Province+City (the location of the cases brought to trial) +Case*," to name the five cases for convenience.

[439] Article 365 of the *Criminal Law of People's Republic of China*: Whoever arranges for pornographic performances shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention or public surveillance and shall also be fined; if the circumstances are serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than ten years and shall also be fined [组织进行淫秽表演的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金].

[440] SHDF NATIONAL OFFICE: *Guang Xi Province: The city of Nan Ning rendered a judgment about online*

As the case was adjudicated after the start of the "CleanNet 2019" campaign, the court reported the case to the SHDF National Office to show their endeavor of implementing the order, which harsh struck the online obscene live streaming of the "CleanNet 2019" issued by the SHDF National Office through punishing the arrangement of a two-day online obscene live show with one-year imprisonment and fines.

Sichuan Leshan Case.[441] On April 30, 2019, in terms of the clues provided by the SHDF National Office, the Bureau of Public Security of Le Shan city of Si Chuan Province investigated a case that refers to disseminate pornography materials online by taking advantage of mobile phone software named "Cat Aggregation Live Streaming Box." Upon investigation, the law enforcement agencies found that the perpetrator, *Zhang*, bought the source code (SC) on the website of Ali Aggregation at the expense of approximately 30,000 yuan. Then, he coordinated and built the App platform of "Cat Aggregation Live Streaming Box" and did the management and maintenance thereof. The users could download the phone App through the web link and register as a member. The member should top up their account and buy the keywords to access the online obscene live shows by Alipay and WeChat Pay[442]. As the case was reported, over 70,000 members registered into the App, and 5,000 of them bought the keywords for accessing the online obscene live shows. More than 130,000 yuan as criminal profits had been collected. Up to May 31, 2019, *Zhang* has been arrested, and the case is still under the process of trial.

Though no exact judicial results are there, this case reveals, from the other side, the massive engagement in online obscene live streaming and the disproportionate ratio of benefits to expenses might stimulate the potential perpetrators to commit the crime of engaging in online obscene live streaming with opportunism.

Zhejiang Jiaxing Case.[443] In June 2019, the Nan Hu District Court of Jia Xing of Zhe Jiang Province announced a case of criminal securing profits by broadcasting online

---

obscene live streaming [广西：南宁市宣判一起网络直播淫秽表演案], 19 June 2019, http://www.shdf.gov.cn/shdf/contents/11420/401368.html

[441] SHDF NATIONAL OFFICE: *Si Chuan: The city of Le Shan investigated a case of utilizing phone software to broadcast online pornographic live shows* [四川：乐山市查办一起利用手机直播软件进行网上传播淫秽色情案件], 31 May 2019, http://www.shdf.gov.cn/shdf/contents/11419/401357.html

[442] *Alipay* and *WeChat Pay* are two of the most popular online payment methods in China of which the previous subjects to *Alibaba Inc* and the latter belongs to the *Tencent Inc.* Their functions are akin to the *PayPal.*

[443] SHDF NATIONAL OFFICE: *Zhe Jiang: The court in the city of Ja Xing adjudicated a case of making criminal profits by disseminating online pornography through the Nebula Platform* [浙江：嘉兴市"星云直播"平台传播淫秽物品牟利案宣判], 17 June 2019, http://www.shdf.gov.cn/shdf/contents/11420/399777.html

pornographic live shows through an online live streaming platform, Nebula Platform. There were seven perpetrators involved in this case. The court sentenced two of the defendants, *Yue Mou* and *Liu Mou*, to imprisonment with 3-year-and-6-month and 3-year-and-3-month periods and a fine of 50,000 yuan and 45,000 yuan. The other five defendants, *Yang Mou*, *Luo Mou*, *Zhao Mou Tian*, *Jiang Mou Na*, and *Zhao Mou*, were sentenced commensurate with their scenarios in the crime. According to the facts part of the judgment, the court found that from August 2017 to December 2017, *Yue Mou* and *Liu Mou* directly bought Nebula Live Streaming Platform from others and arranged amounts of female hosts to perform online obscene live shows. *Yang Mou* funded the platform's technical maintenance. *Luo Mou* was employed to manage the Nebula Platform. *Zhao Mou Tian*, *Jiang Mou Na*, and *Zhao Mou* were responsible for managing female hosts pertained to them as patriarchs. As the case was reported on December 12, 2017, the Nebula Platform accumulated criminal profits of more than 800,000 yuan, and the record of member registration was over 60,000 pieces.

This case is similar to the *Guangxi Nanning Case* above, so it was reported to the SHDF National Office. (The trial took place after the CleanNet 2019 began.) However, this case has some unique features that need to be mentioned. First are the perpetrators involved in this case belong to the circumstance of multi-perpetrators. It is a joint crime with principals and accomplices. Second, it is an organized crime committed by a gang of seven members. Amongst the crime, each of the perpetrators contains a clear division of labor cooperations and thus indicates the complexity of the issue of online obscene live streaming. It is not a simple cybercrime in some situations, but instead, to some extent, an intricate cybercrime with the characteristics of organized crime committed by gangs.

Jiangxi Jiujiang Case.[444] In June 2018, the SHDF Office of De An Country of the city of Jiu Jiang received some clues from the masses about which an online live streaming platform called "You Jiang" has female hosts who performed pornographic live shows and made criminal profits by the reward gifts from the audience. Furthermore, the platform did pimp for their audience at the same time. After receiving whistle-blowing, the SHDF Office of De An Country instantly coordinated and organized the local law enforcement agencies for a special working group, a "6.05" working group. After the preliminary technical investigation and fixing evidence, the "6.05" working group started a formal investigation on

[444] SHDF NATIONAL OFFICE: *Jiang Xi: The court in the city of Jiu Jiang sentenced the '6.05' case of gaining criminal profits by disseminating online pornography through an online live streaming platform* [江西：九江市判结"6•05"网络直播平台传播淫秽物品牟利案], 19 September 2019, http://www.shdf.gov.cn/shdf/contents/11419/405296.html

June 19, 2018. Upon the investigation, the working group found that the platform took advantage of different fake names to escape investigation, and, at the same time, it convened hundreds of female hosts across the China mainland to engage in the online obscene live shows. This platform has a stringent organizational hierarchy. All the hosts on this platform had their group, which a group leader manipulated. The group leader facilitated the hosts to withdraw money from the platform and promoted the communication between the platform manager and hosts. With further evidence securing, the working group locked on two female hosts, *Song Mou Mou* and *Zhan Mou Mou*, on the platform and arrested them separately in Ningbo city of Zhejiang Province and Xingzi city of Jiangxi Province on August 18, 2018. By interrogating two hosts thereinto, they confessed to two group leaders, *Wei Mou Mou* and *Zhi Mou Mou*. On September 18, 2018, the working group arrested six group leaders in six different provinces in China's mainland, namely Yunnan, Shaanxi, Shandong, Guangdong, Hainan, and Anhui Province. The working group found another group leader in Hainan province during the next interrogation and finally arrested him. On July 29, 2019, after trial by the De An County Court, nine perpetrators in total were sentenced to fixed-term imprisonment ranging from five months to one year, and the total amount of fines and penalties was more than 257,000 yuan by citing Article 363 of the Criminal Law of the People's Republic of China (Crime of Producing, Reproducing, Publishing, Selling, or Disseminating Obscene Materials for Making Profits [制作、复制、出版、贩卖、传播淫秽物品牟利罪]).[445]

This case is a typical case related to online obscene live streaming with some peculiarities. First, though many perpetrators are involved in this case, it is not a gang crime compared with the *Zhejiang Jiaxing Case*. All the perpetrators committed the same crime separately but used the same platform. Second, in this case, the platform applied a stringent organizational hierarchy to achieve effective and relatively safe management for the general operation. Third, in this case, the platform had formed a fairly mature industrial chain to

[445] See. Article 363 of *the Criminal Law of the People's Republic of China*: Those producing, reproducing, publishing, selling, or disseminating obscene materials with the purpose of making profits are to be sentenced to three years or fewer in prison or put under limited incarceration or probation, in addition to paying a fine. If the case is serious, they are to be sentenced to three to 10 years in prison in addition to having to pay a fine. If the case is especially serious, they are to be sentenced to 10 years or more in prison or given life sentence, in addition to a fine or confiscation of property [以牟利为目的，制作、复制、出版、贩卖、传播淫秽物品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金；情节特别严重的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产].

some extent. The well-designed process of money withdrawing, hosts enrolling, and communication, to a degree, ensure the secrecy of the management behind the platform and the "security" (not realized by law enforcement agencies) of the platform itself. The last, this case involved many geographical areas showing the trend of the cross-regional feature (even though the regions, in this case, are all in China mainland) of online obscene live streaming.

Hubei Macheng Case.[446] On April 30, 2019, the Public Security department of Macheng city of Hubei Province successfully arrested and repatriated the principals, *Hong Mou Mou* and *Li Mou*, who absconded from Mongolia to the Philippines after reported to the law enforcement agency of the case of disseminating pornography materials online; thoroughly destroyed a criminal gang of committing cybercrime cross-national under the guise of an online-game company; closed down six domestic online obscene live streaming platform; arrested another 20 members of the criminal gang aforementioned with support of the Bureau of International Cooperation of the Ministry of Public Security of China and the law enforcement agencies of Philippine, under the instruction of Ministry of Public Security of China and Office of the "CleanNet 2019" campaign of Provincial Bureau of Public Security of Hubei Province.

In March 2018, the police of public security in the city of Macheng of Hubei got a clue from the whistle-blower, and in the early investigation, found that some users distributed QR (Quick Respond) code for downloading an App software for online obscene live streaming called "Huahua Platform." The users should download and install the App on their mobile terminal and register in by verifying the phone numbers. When entering into the platform, the users could find many broadcast rooms of obscene live shows. By sending the hosts reward gifts ranging from 0.5 yuan to 1888 yuan, the users could require the host to do different kinds of indecent conduct, even intercourses. On further investigation, the law enforcement found that this platform had a stringent organizational hierarchy of boss, operation and maintenance, advertising promotion, customer service management, payment and settlement, group leader, hosts.

Furthermore, the criminal gang had changed the server and shell of the platform many times to escape the whistle-blowing and investigation. The criminal gang employed particular

[446] SHDF NATIONAL OFFICE: *Hu Bei: The police knocked out the transnational criminal gang of online obscene live streaming. The illegal gains were 16 million, and 20 people were arrested* [湖北：警方打掉跨国网络色情直播团伙 牟利1600万 20人落网], 30 May 2019, http://www.shdf.gov.cn/shdf/contents/11419/400064.html

employees to maintain the server aborad in Mongolia and utilized the foreign bank account to do the money laundering. During the operation of this platform from November 2017 to March 2018, the platform had had over 90,000 registered members and made criminal profits of over 16 million yuan in five months. The law enforcement arrested 18 members of the criminal gang in China mainland and another two principals, *Hong Mou Mou* and *Li Mou*, which got the information of the investigation, escaped from Mongolia to the Philippines via South Korea, and kept doing the same criminal business in Philippine by a new-built platform called "Jinnezha" App Platform, were arrested in the end as referred above.

During the interrogation, law enforcement knew that the suspect *Hong Mou Mou* had a company named "Shanghai Tingyu Network Technology co., LTD" in Shanghai, China, specializing in the development of online games. Because of the depression of business and, therefore, the difficulty of maintaining the company, *Hong Mou Mou* organized his shareholders and employees to engage in the pornographic live streaming business. The case is still under trial now in the Macheng Court of Hubei Province.

This case is relatively complicated when compared with all the examples above, for it encompassed all the features of online obscene live streaming aforementioned, such as multi-perpetrators, labor cooperation, organizational hierarchy, and cross-regional perpetration. However, this case has its uniqueness to be discussed. First, each process of the platform's operation referred to an independent crime, for example, financial accounting with money laundering, product promotion with false advertising, and so on. Second, the remote manipulation of the platform and the aboard server location reveal the transnational feature of the new trend of online obscene live streaming, which calls for international judicial cooperation. Third, the transformation from an online game company to a criminal gang reflects the high-profit margin and the lack of supervision in the online broadcast industry to stimulate more professional and organizational subjects, e.g., legal persons, to engage in the online obscene live streaming business.

2.1.3 Case summary and generalization

The proceeding subsection introduced five cases retrieved from the web page of the SHDF National Office as examples of the so-called achievements of local law enforcement in the "CleanNet 2019" campaign. The five example cases were introduced in a profound logic which from simple to complex. The first case, *Guangxi Nanning Case*, was with a single criminal perpetrator who organized the online obscene live shows. From this case, we could find some traces of the harsh strike requirement made by the SHDF National Office in the

"CleanNet 2019" campaign. The second case, *Sichuan Leshan Case*, had some distinctions with the *Guangxi Nanning Case* that the perpetrators in the *Guangxi Nanning Case* took advantage of the existing live streaming platform to commit the crime; while the perpetrators in the *Sichuan Leshan Case* built the platform by himself, though the Source Code he bought from others. This scenario showed the criminal innovation created by the criminals in the online obscene live streaming. The third case, *Zhejiang Jiaxing Case*, is not a simple case with single suspects but a gang of criminals. It reflects, in the contemporary, the corporate trend of this kind of crime. In the fourth case, *Jiangxi Jiujiang Case*, though many perpetrators were involved, it was not a criminal gang but separately engaged in the obscene live streaming by the same platform. Compared with the first three cases, the mature industry chain first appeared in *Jiangxi Jiujiang Case*, and the cross-regional features remind us of the escalating complexity of such crimes. The last case, *Hubei Macheng Case*, was the most complicated one among these five example cases. It has the characteristics of the first four cases and shows the transnational trend of such crimes on the one hand, and on the other hand, the expansion of the criminal subject from an ordinary natural person to a legal person, the company.

Though insufficient is the small size of samples of five cases, to some extent, as the representative cases reported on the web page of the SHDF National Office, some standard features could still be concluded from the five cases above to grasp the characteristics accurately, developments and some other situations of the crimes as to online obscene live streaming, in other words, generalization.

(1) *High Report from whistleblowers than Police Investigators*. As for a glimpse of five cases, it is easy to find more reports from whistleblowers than police investigators. In other words, most cases of online obscene live streaming come to the attention of law enforcement through whistleblowers reports rather than police investigators. The law enforcement agencies, generally the public security organs in China, found and started investigating the cases related to online obscene live streaming after receiving some tips from the victims or witnesses. Without a doubt, it does not mean those police investigators could not find cases, but under most circumstances, the cases were found through whistle-blowing. It reflects online obscene live streaming as one kind of cybercrime the feature that "cybercrime acts most frequently come to the attention of law enforcement agencies through reports by the individual or corporate victims," as written in the Comprehensive Study on

Cybercrime Report.[447]

However, there are still some divergences. Unlike general cybercrime reported by victims, the audience of online obscene live streaming would be reluctant to report the crime to the law enforcement agencies voluntarily in most cases. It is easy to understand. Then, we need to question the circumstance that the online obscene live streaming had been tipped on. Cases were more likely to be reported by the guardian of the minor audience.[448] As such, online obscene live streaming is suspect of spreading pornography to minors, which is a felony rather than a misdemeanor wherever around the world, according to the different (but with some similarities) legislation.

(2) *Multi-subjects' Engagements*. So-called multi-subjects' engagements in this section refer to many persons involved in the online obscene live streaming both on the perpetrator's side and the audience's side. According to the example cases above, it is easy to recognize the large user group involved in each case. The most significant indicator is the number of registrations of the relative platform, of which 70,000 registrations in the *Sichuan Leshan Case*, 60,000 registrations in the *Zhejiang Jiaxing Case*, and 90,000 registrations in the *Hubei Macheng Case*.

On the one hand, the large user group displays the enormous potentials of the market of online obscene live streaming based on the customers' needs. By the deep consideration of this phenomenon, whether the sweep and broad attitude against all kinds of pornography without any exceptions in China, for example, adult pornography for adult audiences, complies with the natural needs of human beings. It could be arguably said that the contradiction between this unexcepted attack of pornography and the natural needs of human beings gives rise to the high incidence and participation of online obscene live streaming.

On the other hand, as one of the stimuli of committing the relative crime of online obscene live streaming, the large user group, to some extent, impulse the formation of criminal gangs from the single, separated perpetrators. It is a burden to deal with the business of such a large user group, and the perpetrators had to employ other persons to help or

---

[447] STEVEN MALBY, ROBYN MACE, ANIKA HOLTERHOF, CAMERON BROWN, STEFAN KASCHERUS AND EVA IGNATUSCHTSCHENKO (UNODC): *Comprehensive Study on Cybercrime (Draft)*. Vienna, United Nations Office on Drugs and Crime, 2013.

[448] SOHU NEWS: *Juveniles watch pornography on the website. Upload "inventory" to become an administrator* [少年为在网站多看黄片 上传"库存"争当管理员]. *Parents report and expose porn sites to the police* [家长报警曝光黄色网站], 26 October 2019, http://news.sohu.com/20140630/n401556398.shtml

facilitate them. With some organizational rules and labor cooperation, the criminal gang of online obscene live streaming was formed eventually by logic.

(3) *Single-Regional to Cross-Regional to Transnational*. The *Place of Crime*[449] of the online obscene live streaming reflects a trend of transmission from one single region to cross-region, including the transnational region. The cross-regional feature here is not for the users who are, of course, from the multi-geographic areas based on the nature of the Internet, but for the management, operation, and maintenance of the criminal platform and its perpetrators. For escaping the investigation, most members of criminal gangs were better come from different areas and don't know each other, and only some top managers of the platform know who they are and where they are from. Here comes the cross-regional. On the other side, to escape the supervision from the strict Internet control in China, the server of the online platform is better to locate outside of China and best in some countries with different regulations on pornography to China, for instance, see *Hubei Macheng Case*. It is already a popular trend, especially for large-scale crimes, and most of the servers involved are located outside mainland China. It is easily understandable but intricate to solve the problem, which calls for international judicial cooperation and relatively uniform rules on the pornography of both definition and criminalization. Unluckily, the international model provisions have not formed except child pornography, as the situation of general cybercrime.[450]

(4) *Independent Platform and Mobile Termination Popularity*. Online live streaming has already been a mature industry in China. There are many scaled platforms engaged in online live streaming with many users, such as Pepper Webcast (Huajiao Zhibo in Chinese), the most prominent online live streaming platform with over 26.76 million users in June 2019.[451] The Chinese government has enacted a regulation on the governance of online live streaming platforms since November 2016, the *Provisions on the Administration of Internet Live-Streaming Services (hereinafter,* the Provisions*)*. It stipulates many measures for the online live streaming service providers to self-govern the broadcaster and materials on their platform, such as keeping the record of every live streaming for 60 days, implementing the real-name requirement, supervising the materials in the live streaming, and so on.[452] However,

[449] For the definition of the *Place of Crime*, please see Chapter III-5.3.

[450] STEVEN MALBY, ROBYN MACE, ANIKA HOLTERHOF, CAMERON BROWN, STEFAN KASCHERUS AND EVA IGNATUSCHTSCHENKO (UNODC), 2013.

[451] IIMEDIA RESEARCH CENTER, 2019.

[452] See. Article 7, Article 12, and Article 16 of the *Provisions on the Administration of Internet Live-Streaming Services* [互联网直播服务管理规定].

when analyzing the cases above, the perpetrators of online obscene live streaming did not use the popular platform controlled by the network companies but built an independent and secretory platform to commit the crime. Then, the Provisions seems to be invalid to these kinds of platforms specializing in pornography because the preliminary aim of these platforms is to commit crime secretly. They would not follow the rules set in the Provisions. Furthermore, the popularity of mobile termination gives rise to the convenience of spreading the platform and the obscenity therein. So, the independent platform and the popularity of mobile termination, such as Apps, has already been a trend of online obscene live streaming.

(5) *Multi-crimes Involving*. Online obscene live streaming encompasses multi-crimes in general. According to the Criminal Law of China, there are at least four different crimes encompassed at issue. These articles will be introduced in the next section. However, many scholars in China have already realized this problem.[453] Taking the Hubei Macheng Case as an example, the perpetrators would refer to disseminating pornography, false advertisement, illegal use of ICTs, and other crimes. The theoretical questions involved here are Criminal Concurrence and Offenses Counting.[454] The case's complexity challenged the legal reasoning and application of criminal law in the trial. To protect the legality principle of criminal law, some articles demand much more discussion to solve the problem of multi-crimes involved in online obscene live streaming cases, which calls for new legislation or new interpretation to deal with the criminal concurrence and offenses counting.

---

[453] See. BOHAO CAI: Analysis of the Criminal Norm of New Internet Pornography: Based on the Live Broadcasting Obscenity Performance [新型网络色情的刑事规范分析：以直播平台淫秽表演为切入]. *Journal of Heilongjiang Administrative Cadre Institute of Politics and Law* [黑龙江省政法管理干部学院学报], vol. no. 2. (2016) 24-26+30; JIE MEI: *Criminal Regulations on Web Live Video Streaming* [网络直播的刑法规制]. Harbin, China, Heilongjiang University, 2017; YUNXIA PANG AND LI SUN: On Criminal Regulations on Online Obscene Live Streaming [论网络色情直播的刑法规制]. *Journal of Changchun Normal University* [长春师范大学学报], vol. 37. no. 7. (2018) 40-43; YUN TENG: *The Criminal Law Analysis of Internet Pornographic Broadcast* [网络色情直播行为的刑法分析]. Lanzhou, China, Lanzhou University, 2018; GONGZHENG WANG: Criminal Regulation of Erotic Behavior on Live Online Platform [网络直播平台色情行为的刑法规制]. *Journal of Nanjing University of Aeronautics and Astronautics (Social Sciences)* [南京航空航天大学学报（社会科学版）], vol. 20. no. 1. (2018) 52-57.

[454] See. XIANQUAN LIU: On the Theory of Quantity of Crime [罪数形态理论的正本清源]. *Chinese Journal of Law* [法学研究], vol. 31. no. 4. (2009) 122-136; XINGLIANG CHEN: From Offenses Counting to Concurrence: An Academic Advancement [从罪数论到竞合论：一个学术史的考察]. *Modern Law Science* [现代法学], vol. 33. no. 3. (2011) 99-112; MINGKAI ZHANG: Distinctions between the Overlap of Articles of Law and the Imaginative Joiner of Offenses [法条竞合与想象竞合的区分]. *Chinese Journal of Law* [法学研究], vol. 38. no. 1. (2016) 127-147; LINGBO XU: The System Position and Principle of Criminal Concurrence: The German Concurrence Theory as a Reference [犯罪竞合的体系位置与原则：以德国竞合理论为参照]. *Journal of Comparative Law* [比较法研究], no. 6. (2017) 86-97.

2.2 COPING WITH ONLINE OBSCENE LIVE STREAMING IN CHINA

2.2.1 The Principle of Legality in Criminal Law

There are four fundamental principles in modern criminal law, namely, the Principle of Legality, the Principle of Conduct, the Principle of Culpability, and the Principle of Personal Liability.[455] The Principle of Legality has four secondary principles: (I) the principle related to sources of criminal law; (II) the principle related to applicability of the criminal law in time; (III) the principle related to applicability of the criminal law in place; and (IV) the principle related to interpretations of the criminal law.[456]

Principle I aims to address the question of the origin of criminal norms. Usually in European civil law countries, the source of criminal norms comes from written laws enacted by Parliament. In common law countries, criminal norms can also be derived from precedent. At the same time, principle I also requires formal publicity of criminal norms. Only formally publicized criminal norms can fairly ensure that citizens comply efficiently with them.[457]

Principle II aims to address the question of the temporal effects of criminal norms. Principle II has three requirements. First, the old criminal norms are superior to the application of the new criminal norms, that is, the criminal law at the time of the crime is applied to the criminal case. Second, procedural criminal norms apply to all judicial rulings from the date of entry into force. The third is to give priority to the application of mitigating substantive criminal norms to handle criminal cases.

Principle III aims to address the question of the spatial validity of criminal norms. Principle III has two requirements. First, procedural criminal norms apply to any judicial decision that is considered domestic. The second is the domestic factual events in which domestic substantive criminal norms apply to domestic decisions. In addition, domestic substantive criminal norms apply in accordance with domestic interests to foreign factual events decided in the country on the basis of lawful extraterritorial applicability (protective, passive, active or universal).[458]

Principle IV aims to address the issue of interpretation of criminal norms. The interpretation of criminal norms generally has two stages. The first stage is the formulation of

[455] See. GABRIEL HALLEVY: *A Modern Treatise on the Principle of Legality in Criminal Law*. Heidelberg, Springer, 2010, p. 4.
[456] See. GABRIEL HALLEVY, 2010.
[457] See. GABRIEL HALLEVY, 2010, pp. 16-46.
[458] See. GABRIEL HALLEVY, 2010, pp. 49-78.

criminal norms. The formulation stage of criminal norms refers to the stage when an organ with the legislative authority formulates criminal law. There are three main requirements for the interpretation of criminal law at this stage: First, generality. Criminal law norms must be directed at unspecified individuals. The second is feasibility. Criminal law norms must be able to be enforced with the possibility and practicality of their application. The third is clarity and precision. Criminal law norms that are too vague are invalid (Void-for-Vagueness).[459]

The second stage is the application of criminal norms. The stage of application of criminal law norms usually refers to the stage in which the court implements and interprets criminal law in judicial practice. The criminal law interpretation at this stage mainly involves the following contents: First, strict interpretation, that is, during the effective period of the criminal law norms, the court must make convictions and sentencing in strict accordance with the provisions of the criminal law. The second is the purposive interpretation, that is, when the verbal logic of the current criminal norms does not adapt to their legal logic, the court can apply the criminal norms by reasoning to the legislative purpose. Third, analogical interpretation is strictly prohibited.[460]

Some scholars believe that the principle of *Nulla poena sine lege* (no penalty without law) is equivalent to the principle of legality.[461] However, this subsection argues that this recognition is insufficient. Principle of *Nulla poena sine lege* has four subordinate principles[462], which correspond to partial contents of Principle of Legality: (1) *Nulla poena sine lege praevia* (no penalty without previous law) which prohibits ex post facto laws corresponds to the Principe II of the Principle of Legality; (2) *Nulla poena sine lege scripta* (no penalty without written law) which excludes customary law corresponds to the Principle I of the Principle of Legality; (3) *Nulla poena sine lege certa* (no penalty without well-defined law) which rejects the vagueness of law corresponds to the requirement of Clarity under the Priciple IV of the Principle of Legality; and (4) *Nulla poena sine lege stricta* (no penalty without exact law) which prohibits analogical interpretation corresponds to the requirement

[459] See. GABRIEL HALLEVY, 2010, pp. 92-129; JAMES J. SPIGELMAN: The Principle of Legality and the Clear Statement Principle. *Australian Law Journal*, vol. 79. (2005) 769.

[460] See. GABRIEL HALLEVY, 2010, pp. 133-163.

[461] See. e.g., DOUGLAS N. HUSAK AND CRAIG A. CALLENDER: Wilful Ignorance, Knowledge, and the Equal Culpability Thesis: Study of the Deeper Significance of the Principle of Legality. *Wisconsin Law Review*, vol. 1994. no. 1. (1994) 29-70; LI LI: Nulla Poena Sine Lege in China: Rigidity or Flexibility. *Suffolk University Law Review*, vol. 43. no. 3. (2010) 655-668.

[462] See. JEROME HALL: Nulla Poena Sine Lege. *The Yale Law Journal*, vol. 47. no. 2. (1937) 165-193.

in Principle IV.

2.2.2 Substantial Regulations on Online Obscene Live Streaming

Substantial regulations on online obscene live streaming are composed of hierarchical regulations, such as law, administrative regulations, and departmental acts. Furthermore, the judicial interpretation of the law casts a significant role in the criminal justice system. This section will predominantly focus on criminal law and its judicial interpretations.

In the Criminal Law of China, there are no articles specialized in online obscene live streaming. The regulations are generally stipulate all types of pornography or obscenity. There is an independent section in regulating pornography, namely Article 363, which focuses on making criminal profits from producing, duplicating, publishing, selling, disseminating pornographic or obscene materials, and offering book numbers for the publication of pornographic books and journals; Article 364, which focuses on the general disseminating of pornography and obscenity, and organizing and playing obscene or pornographic audio/video materials; Article 365, which focuses on the organizing the pornographic or obscene shows; Article 366, which focuses on the legal person's culpability when committing the crimes of this section; and Article 367, which defines pornographic or obscene materials in these articles. There is another article that needs to be mentioned here is that Article 301 focuses on group-sexual behaviors. Some scholars hold the view that the broadcaster of obscene live shows violated Article 301 at the same time.[463]

Despite the Criminal Law, there are four documents related to the online obscene live streaming, of which one is the decision, and the other three are judicial interpretations. With the consideration of online disseminating pornography, the Standing Committee of the National People's Congress of China decided to govern this kind of problem in 2000. This decision, at first, was not to focus on the online obscene live streaming but general rules on regulating the increasingly rampant online disseminating pornography.[464] Later in 2004 and 2010, the Supreme People's Court and the Supreme People's Procuratorate enacted a judicial interpretation that detailed the application of the Criminal Law on pornography in cyberspace.[465] Meanwhile, the Supreme People's Procuratorate and Ministry of Public

[463] JIE MEI, 2017; YUN TENG, 2018.

[464] See. Article 3 (5) of the *Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security* [全国人民代表大会常务委员会关于维护互联网安全的决定]

[465] See. *Interpretation on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations* [最

Security promulgated another judicial interpretation that focuses on the specific rules and standards of filing a case related to law enforcement agencies.[466]

2.2.3 Procedural and Evidential Regulations

The crime of online obscene live streaming is a kind of cybercrime in nature. The evidential and investigatory laws and rules applied to online obscene live streaming are ultimately applied to cybercrime. "Several countries outside of Europe do not admit electronic evidence at all, making the prosecution of cybercrime, and any other crime evidenced by electronic information, unfeasible."[467] However, China has already admitted the status of the electronic data produced in online activities as the legal form of evidence in establishing the facts relevant to guilt or innocence of an individual at trial by Article 50 of the Criminal Procedure Law of China.[468] Due to the particularity of cybercrimes involving electronic data, the Criminal Procedure Law of China [469] and the Ministry of Public Security[470] also stipulate that electronic data can be obtained through Technical Investigation Measures. Technical Investigation Measures are commonly referred to as Digital Forensics. It

---

高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释] and *Interpretation (II) of Several Issues on the Specific Application of Law in the Handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornographic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations* [最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二)].

[466] See. *Provisions (I) on the Standards for Filing Criminal Cases under the Jurisdiction of the Public Security Organs for Investigation and Prosecution* [关于公安机关管辖的刑事案件立案追诉标准的规定(一)].

[467] STEVEN MALBY, ROBYN MACE, ANIKA HOLTERHOF, CAMERON BROWN, STEFAN KASCHERUS AND EVA IGNATUSCHTSCHENKO (UNODC), 2013.

[468] Article 50 of *Criminal Procedure Law of the People's Republic of China*: All materials that may be used to prove the facts of a case are evidence. Evidence includes: […] (8) audio-visual recordings and electronic data. […]. [可以用于证明案件事实的材料，都是证据。证据包括： […]（八）视听资料、电子数据[…].]

[469] See. Article 150 of *Criminal Procedure Law of the People's Republic of China*: After filing a case regarding […] any other crime seriously endangering the society, a public security authority may, as needed for criminal investigation, take technical investigation measures after undergoing strict approval formalities. [公安机关在立案后，对于[…]其他严重危害社会的犯罪案件，根据侦查犯罪的需要，经过严格的批准手续，可以采取技术侦查措施。]

[470] See. Article 254 of *Provisions on the Procedures for Handling Criminal Cases by Public Security*: After the case is filed, the public security organ may, according to the needs of investigating crimes, take technical investigation measures against the following criminal cases that seriously endanger the society: […] (4) major criminal cases committed through telecommunications, computer networks, delivery channels, etc., as well as major criminal cases committed against computer networks. […]. [公安机关在立案后，根据侦查犯罪的需要，可以对下列严重危害社会的犯罪案件采取技术侦查措施: […]（四）利用电信、计算机网络、寄递渠道等实施的重大犯罪案件，以及针对计算机网络实施的重大犯罪案件；[…]。]

existed in the investigation process and was manipulated by law enforcement agencies, the Public Security Organs in China. After obtaining the electronic data, in general, both Procuratorate and Court would scrutinize the evidence's authenticity, legality, and relevance. To further standardize the collection and examination of electronic data as evidence, the Ministry of Public Security, Supreme People's Procuratorate, and Supreme People's Court have formulated two judicial interpretations[471] respectively to guide relevant work.

2.3 DISCUSSIONS: PROBLEMS IDENTIFIED AND STRATEGY CHOICES

2.3.1 Online obscene live streaming and Sexting

"Sexting, the portmanteau of Sex and Texting, has become a hot topic of debate between the legislators, researchers, educators, parents, and teens."[472] Generally, sexting means receiving and sending sexually explicit materials through electronic means, especially cell phones.[473] Marcum, Higgins, and Ricketts, and Hasinoff believed that sexually explicit materials just included personal photos and texts.[474] However, in light of technology development, the scope of sexually explicit materials should expand to include videos, audio messages, and some other forms of materials.[475]

When looking back at online obscene live streaming, the host[s] or broadcaster[s] would broadcast obscene shows including but not limited to sexual intercourse, masturbation, and other materials arising from prurient interests. Online obscene live streaming, in nature,

---

[471] See. e.g., *Provisions on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases* (01 October 2016) [关于办理刑事案件收集提取和审查判断电子数据若干问题的规定]; *Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases* (01 February 2019) [公安机关办理刑事案件电子数据取证规则]; Provisions on the Handling of Cybercrime Cases by People's Procuratorates (22 January 2021) [人民检察院办理网络犯罪案件规定].

[472] KARUPPANNAN JAISHANKA: Sexting: A new form of Victimless Crime? *International Journal of Cyber Criminology*, vol. 3. no. 1. (2009) 21-25; FAWN NGO, KARUPPANNAN JAISHANKAR AND JOSE R. AGUSTINA: Sexting: Current Research Gaps and Legislative Issues. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 161-168.

[473] DANIELLE M. CRIMMINS AND KATHRYN C. SEIGFRIED-SPELLAR: Adults who Sext: Exploring Differences in Self-Esteem, Moral Foundations, and Personality. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 169-182.

[474] CATHERINE D. MARCUM, GEORGE E. HIGGINS AND MELISSA L. RICKETTS, 2014; AMY ADELE HASINOFF: Sexting and Privacy Violations: A Case Study of Sympathy and Blame. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 202-217.

[475] AMY ADELE HASINOFF, 2017; MARA MORELLI, DORA BIANCHI, ROBERTO BAIOCCO, LINA PEZZUTI AND ANTONIO CHIRUMBOLO: Sexting Behaviors and Cyber Pornography Addiction Among Adolescents: The Moderating Role of Alcohol Consumption. *Sexuality Research & Social Policy*, vol. 14. no. 2. (2017) 113-121; JOANNE SWEENY AND JOHN SLACK: Sexting as 'Sexual Behavior' Under Rape Shield Laws. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 246-260.

is disseminating pornography or obscenity by online live streaming or webcast, whether voluntarily or for other purposes, such as self-display, satisfying sex addiction[476], or gaining criminal profits. It has some similarities to sexting. In this part, it is considered that it belongs to one of several forms of sexting.

Though welcome is sexting among teenagers according to some researches[477], then it is hard to say that, under the circumstance of China's situation of the large users' group of online obscene live streaming, which could be inferred from the five example cases, minors or teenagers are not involved in. Some cases in China have already shown the minors or teenagers involved, and merely, there are no statistics to show the proportion of minors participating. When both audience and broadcasters of online obscene live streaming are minors, it refers to sexting in the context of previous researches out of China. Usually, outside of China, if pornography does not involve minors or children, it will be protected under the protection of free speech. Therefore, distinguishing the different types of obscenity (mainly to see the production, duplication, or dissemination of the whole process of involved material and whether the content itself contains children or minors) is the first task to deal with sexting or obscenity.

In addition, according to the unique feature of forbidding obscenity unexceptionally in China, online obscene live streaming research is a little different from sexting. Nevertheless, the harmfulness, extensive participation of teenagers or minors, and other reasons for the criminalization of sexting, which had been testified and demonstrated in the sexting research, could be learned for the research of online obscene live streaming in the context of China. Notably, so too is of cybercrime, the problems of criminalization, investigation, prosecution,

---

[476] See. KATHRYN SEIGFRIED-SPELLAR: Individual Differences of Internet Child Pornography Users: Peculiar Findings in a Community-Based Study. *International Journal of Cyber Criminology*, vol. 7. no. 2. (2013) 141-154; INGELA LUNDIN KVALEM, BENTE TRÆEN AND ALEX IANTAFFI: Internet Pornography Use, Body Ideals, and Sexual Self-Esteem in Norwegian Gay and Bisexual Men. *Journal of Homosexuality*, vol. 63. no. 4. (2016) 522-540; JOSEPH M. SIRIANNI AND ARUN VISHWANATH: Problematic Online Pornography Use: A Media Attendance Perspective. *The Journal of Sex Research*, vol. 53. no. 1. (2016) 21; RAFAEL BALLESTER-ARNAL, JESUS CASTRO CALVO, M. DOLORES GIL-LLARIO AND BEATRIZ GIL-JULIA: Cybersex Addiction: A Study on Spanish College Students. *Journal of Sex and Marital Therapy*, vol. 43. no. 6. (2017) 567-585.

[477] See. CATHERINE D. MARCUM, GEORGE E. HIGGINS AND MELISSA L. RICKETTS, 2014; KATHY MARTINEZ-PRATHER AND DONNA M. VANDIVER: Sexting among Teenagers in the United States: A Retrospective Analysis of Identifying Motivating Factors, Potential Targets, and the Role of a Capable Guardian. *International Journal of Cyber Criminology*, vol. 8. no. 1. (2014) 21-35; ALISON MARGANSKI: Sexting in Poland and the United States: A Comparative Study of Personal and Social-Situational Factors. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 183-201.

and adjudication existed in sexting are the general problems in online obscene live streaming.

2.3.2 Problems Identified in General in China: Proactive Investigation and Crime Prevention

To summarize the sections above and begin this section, it is clear that online obscene live streaming is illegal in China with a broad and sweeping attitude against all kinds of pornography. The existing regulations, whatever legislations or judicial interpretations, justify the criminal justice system to cope with or deal with this arising problem in cyberspace with huge user groups. The "CleanNet 2019" campaign, carried out by the SHDF National Office, is merely to speed up the centralized rectification of this problem in a specific period, to accurately crackdown, strictly control or even eliminate, the result of which is often accompanied by the more massive application of penalties. However, is the approach of China on combatting online obscene live streaming unquestionable? The answer to this question is definitely no. After all, like Case, Johnson, Manlow, Smith, and Williams had written in their book, "[R]ecognition that there is no ideal is an important aspect of life and justice."[478]

As discussed above, cybercrime cases are more likely to be reported by victims, though the low rate is the report of an individual or corporate victim for fear of shame, embarrassment, and detrimental evaluations. In re cases of online obscene live streaming, in most situations without minors or children involved, are enduring lower report rate of the audience (compared with higher report rate of the whistleblower) for consistent needs dwelling on accessing obscenity.

On the other hand, because of the particularity of transmission of obscenity or pornography at an online live streaming platform, such as there is no physical material existed, and all the information transmitted will be deleted soon after shutting down the live streaming, the cross-regional or transnational feature. The convenience of accessing online obscene lives generated by popular uses of mobile termination, the mobile phone Apps, is problematic for law enforcement agencies to enact proactive investigation measures. Traditional investigatory measures by which law enforcement agencies take, such as data interception, metadata analysis, sensitive words recognition, and other measures recommended by AÇAR in his paper[479], on one side, are based on the cooperation of Internet

[478] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS: *Criminology*. New York, Oxford University Press, 2017.

[479] KEMAL VELI AÇAR: Webcam Child Prostitution: An Exploration of Current and Futuristic Methods of Detection. *International Journal of Cyber Criminology*, vol. 11. no. 1. (2017) 98-109.

companies or platforms. However, as discussed above, the online platform specializing in disseminating obscenity prongs not assist and cooperate with the law enforcement agencies to fulfill the investigation. In general, they are trying to escape it.

On the other side, these measures belong to methods of detection *ex post facto*. In other words, the application of these measures happened after the crime had been reported to law enforcement agencies rather than providently employed, thereby preventing the crimes. In addition, even if these investigation methods are adopted after reporting, it is impossible to guarantee that these crimes can be adequately detected due to the difficulty in the investigation of cybercrimes and the secrecy of the online obscene live streaming platform, let alone the effectiveness and sufficiency of these methods as crime prevention.

Then, by putting the low report rate and the after feature, effectiveness, and sufficiency of measures of cybercrime detection together into the examination of situational crime prevention theory, which is "[b]ased on a range of theories about the process leading to the commission of crime described as 'opportunity theories,' consisting of 'the rational choice perspective, the routine activity approach, and crime pattern theory,'" it could be found that the features of the online obscene live streaming platform as generalized before, such as easy to build a live streaming platform, high reward rate, expansive engagement of users, the convenience provided by mobile phone Apps, and uneasy about being discovered and investigated, totally hinder the function of crime prevention within the theory of situational crime prevention which calls on "reducing opportunity, creating inhibitor, and creating more considerable uncertainty as to the outcomes of crime (greater risk/lower rewards)."[480] As such, proactive crime prevention of online obscene live streaming seems to be invalid under these circumstances. However, this is not the problem that just exists in China but worldwide in dealing with cybercrime.

2.3.2 Problems Identified in Particular in China: Clarification, Unification, and Standard

As mentioned previously, the Principle of Legality in criminal law has numerous derivative principles. Together, they define the meaning of the Principle of Legality in criminal law. Suppose China's governance of online obscene live streaming was in line with the requirements of the Principle of Legality in criminal law. In that case, it should adhere to all derivative principles thereof. Suppose some of the derivative principles of the Principle of Legality in criminal law had not been well implemented in China's governance of online

[480] See. STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS, 2017.

obscene live streaming. In that case, it could be said that China's governance of online obscene live streaming does not fully adhere to the Principle of Legality in criminal law. Based on this reasoning, this article argues that China's online obscene live streaming governance does not fully adhere to the Principle of Legality in criminal law. It manifests in the following three areas:

First, in China's judicial practice, the practice of identifying online obscene live streaming as obscene information is debatable.

In terms of online obscene live streaming, the keyword is obscene or obscenity. The definition of obscenity is vital to the measures taken to deal with the problem. In Chinese criminal law, crimes of obscenity, besides the *Crime of Organizing Pornographic Performance* [组织淫秽表演罪] in Article 365, incorporate the terminology of Obscene Material [淫秽物品]. Article 367 affords the definition of Obscene Material: "Obscene materials mentioned in this law refer to erotic books, magazines, motion pictures, videotapes, audiotapes, pictures, and other obscene materials that graphically describe sexual intercourse or explicitly publicize pornography. […]"[481]

By analyzing Article 367, we could find an essential requirement of the obscene materials, which is of physical form thereof. Judicial interpretations classify obscene electronic information as other obscene materials.[482] Criminal justice needs evidence to determine whether a piece of information is obscene. Article 50 of China's Criminal Procedure Law recognizes audio-visual materials and electronic data as legal forms of evidence. However, if obscene information is to be used as evidence for a verdict, it must be fixed in audiovisual or electronic data or other forms. In other words, although the Criminal Procedure Law stipulates those audio-visual materials and electronic data are legal forms of evidence, they must be able to be fixed to prove the case.

---

[481] Chinese version: 本法所称淫秽物品，是指具体描绘性行为或者露骨宣扬色情的诲淫性的书刊、影片、录像带、录音带、图片及其他淫秽物品。

[482] See Article 9 of the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations* [最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释]: The "other pornographic articles" as prescribed in paragraph 1 of Article 367 of the Criminal Law shall include […] other electronic information of internet and terminal of mobile communications […] [刑法第三百六十七条第一款规定的"其他淫秽物品"，包括[…]互联网、移动通讯终端电子信息[…]].

Online live streaming is officially defined as "the activities of continuously releasing real-time information to the public based on the Internet in such forms as videos, audio, images and texts."[483] Accordingly, online obscene live streaming shall refer to live streaming with sexual arousal as the purpose or means, the Internet as the carrier, and obscenity/pornography as the content. The operation of online live streaming is technically achieved through the iteration of data.[484] The content of the current second is stored, and the content of the subsequent second will replace the content of the previous second. The repetition of this process ensures that the live streaming is carried out. This is a dynamic process, not an objective reality presented statically. At the technical level, countless electronic data was born and disappeared, rather than one electronic data constantly changing. In addition, live streaming is still live streaming without data and can be carried out with or without technical support. Face-to-face live streaming is transmitted through the medium of air and light. Live television streaming is transmitted through signals. Online live streaming is transmitted through electronic data. Data is a medium, not a vehicle. Therefore, in essence, online obscene live streaming cannot be identified as fixed electronic information (consisting of electronic data). Because data is only the medium of information, and live streaming is an act of disseminating information. This behavior generates data on the Internet, which does not mean that this behavior is data. Furthermore, if live online obscene live streaming cannot be considered electronic information, it cannot be considered obscene materials. Further, it is not a constituent element of the crime of obscenity in China's criminal law.

It is worth noting that the inability to identify an online obscene live streaming as obscene information (obscene material) does not mean that it is innocent. It is only through the verbal logic of criminal norms that the expansion of online obscene live streaming to obscene materials does not conform to the Strict Interpretation Principle within the Principle of Legality in criminal law. There are other crimes in China's criminal law that can deal with this situation, such as the *Crime of Gathering a Crowd for Promiscuous Activities* [聚众淫乱罪].[485] The *Crime of Gathering a Crowd for Promiscuous Activities* punishes the behavior of

[483] See, Article 1 of the Provisions on the Administration of Internet Live-Streaming Services [互联网直播服务管理规定]

[484] WEI ZHU: Research on the Progress of Internet Broadcast Technology [互联网直播技术研究]. *Modern Information Technology* [现代信息科技], vol. 2. no. 10. (2018) 104-106.

[485] Some Chinese scholars held the viewpoint that the Crime of Gathering a Crowd for Fornication might be more proper for dealing with online obscene live streaming. See. e.g., BOHAO CAI, 2016, p. 25; YU XIA AND GUOQIANG LIU: The Criminal Regulations of the Internet Pornography Live Broadcast [论网络色情

gathering a crowd for promiscuous activities.[486]

Second, even if online obscene live streaming is identified as obscene information, there is a situation where a judicial determination is inconsistent in China's judicial practice.

For example, in the Guangxi Nanning Case cited in this chapter, the perpetrator was convicted of the *Crime of Organizing Pornographic Performance*. In the Jiangxi Jiujiang Case, the perpetrator was convicted of the *Crime of Producing, Reproducing, Publishing, Selling, or Disseminating Obscene Materials for Making Profits*. There are many more cases of this divergence. One study showed that as of March 2019, researchers had retrieved a total of 33 cases related to online obscene live streaming on *China Judgements Online* [中国裁判文书网]. These cases were either decided by the *Crime of Disseminating Obscene Materials* or by the *Crime of Organizing Pornographic Performance* and to some extent, there were inconsistencies in their evaluation criteria.[487] In Zhao Mou's Case, the offender who conducted online obscene live streaming on live streaming platforms and guided viewers to swipe gifts for profit was convicted and punished for the *Crime of Disseminating Obscene Materials for Making Profits.*[488] However, in Feng Mou's Case, the offender purchased other persons' identity information to register social accounts and purchased live streaming systems, used social platforms to recruit broadcasters to conduct online obscene live streaming, distributed the proceeds proportionally with the broadcasters, and was convicted and punished for the *Crime of Organizing Pornographic Performance.*[489] The perpetrators in both cases were involved in the use of online obscene live streaming for profit but were convicted of different charges. The above cases show that courts in different regions of China have not uniformly characterized online obscene live streaming. These inconsistent determinations, to some extent, violate the requirement of clarity and precision in the

直播行为的刑法规制]. *Journal of Hubei Engineering University* [湖北工程学院学报], vol. 42. no. 1. (2022) 95-101.

[486] See. Article 301 of the Criminal Law of the People's Republic of China: Whoever takes a lead in assembling a crowd to engage in promiscuous activities or repeatedly participates in such activities is to be sentenced to not more than five years of fixed-term imprisonment, limited incarceration, or probation [聚众进行淫乱活动的，对首要分子或者多次参加的，处五年以下有期徒刑、拘役或者管制].

[487] BOYA YU: *A Qualitative Research on Related Offences of Obscene Live Streaming* [互联网淫秽直播相关行为定性研究]. Wuhan, China, Wuhan University, 2022.

[488] See. Zhao Mou's first-instance criminal verdict on the *crime of producing, reproducing, publishing, selling, and disseminating obscene materials for profit* [赵某制作、复制、出版、贩卖、传播淫秽物品牟利罪一审刑事判决书]. Case No. （2018）苏 0213 刑初 71 号.

[489] See. Feng Mou's first-instance criminal verdict on the *Crime of Organizing Pornographic Performance* [冯某组织淫秽表演罪一审刑事判决书]. Case No.（2018）豫 0204 刑初 90 号.

Principle of Legality in criminal law. Because it hinders citizens' prediction of the likely outcome of similar behavior. In turn, they produce ambiguity at the stage of the application of criminal law.

Third, even if focus on a specific offense, China's criminalization criteria for online obscene live streaming are debatable.

The judicial interpretation stipulates that the actual number of clicks on obscene electronic information that was produced, copied, published, sold, or disseminated more than 5,000 or 10,000 times constitutes a crime.[490] This article aims to criminalize the dissemination of obscene information that reaches a relatively wide range of dissemination. In other words, disseminating obscene information without a certain wide scale of dissemination does not constitute a crime. This article generally stipulates the number of clicks on online obscene information as a criterion for criminalization, without taking into account the particularity of online obscene live streaming. Online obscene live streaming relies on online live streaming platforms. There are many live streaming rooms on a live streaming platform. In reality, there are these situations: the user just clicked into the live streaming room but did not watch the subsequent obscene live streaming content; or, the user clicked into the room but the obscene part did not start to perform or spread. In these cases, if

[490] See. Article 1 of the *Interpretation (II) of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations* [最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释(二)]: In case anyone who makes, reproduces, publishes, sells or spreads pornographic electronic information for seeking profits by means of the internet or terminal of mobile communications, and has any of the following circumstances, he shall be convicted and punished as the crime of making, reproducing, publishing, selling and spreading pornographic articles for seeking profits in accordance with the provisions of paragraph 1 of Article 363 of the Criminal Law: [...] (4) The pornographic electronic information made, copied, published, sold or spread by him is clicked for more than 5 thousand times; [...]. [以牟利为目的，利用互联网、移动通讯终端制作、复制、出版、贩卖、传播淫秽电子信息，具有下列情形之一的，依照刑法第三百六十三条第一款的规定，以制作、复制、出版、贩卖、传播淫秽物品牟利罪定罪处罚：[...]（四）制作、复制、出版、贩卖、传播的淫秽电子信息，实际被点击数达到五千次以上的；[...].]; Article 3: If anyone spreads pornographic electronic information by means of the internet or terminal of mobile communications not for seeking profits, and has any of the following circumstances, he shall be convicted and punished as the crime of spreading pornographic articles in accordance with the provisions of paragraph 1 of Article 346 of the Criminal Law: (1) 1. The quantity has reached to two times the standards as prescribed in Item (1) to (5) of paragraph 1 of Article 1 or more; [...]. [不以牟利为目的，利用互联网或者移动通讯终端传播淫秽电子信息，具有下列情形之一的，依照刑法第三百六十四条第一款的规定，以传播淫秽物品罪定罪处罚：（一）数量达到第一条第一款第(一)项至第(五)项规定标准二倍以上的; [...].]

only the number of clicks is used as a criminalization criterion, it seems that it is not in line with the original intent of the legislation. The original intention of the legislation was to combat the dissemination of a certain scale. This scale is mainly reflected in the size of the audience. What reflects the scale of online obscene live streaming in essence should be the number of viewers at the same time, that is, the number of simultaneous viewers. The reality is that China's current criminal normative system does not explicitly use "the number of simultaneous viewers" as the criterion for conviction and punishment. When hearing a case, judges can only mechanically apply the formal standard of "number of clicks" stipulated in the judicial interpretation, while ignoring the substantial standard of "number of simultaneous viewers". Therefore, it can be said that, to some extent, the provisions of judicial interpretation seem to be contrary to the purpose of the legislation. That is, to punish online pornographic crimes that reach a certain scale of dissemination. Furthermore, to some extent, it violates the requirement of Strict Interpretation in the Principle of Legality in criminal law, that is, the interpretation of the criminal norms should conform to the original intent thereof.

2.3.4 Strategy Choices

Based on the above discussion, we seem to have entered a dilemma. On the one hand, according to the legal logic of criminal law, online obscene live streaming needs to be criminalized and imposed; on the other hand, the Principle of Legality in criminal law should bind police, prosecutors, and judges to handle crime control by handling relevant cases. Some Chinese scholars believe that it is possible to break through the predicament by exploring the purpose of the legislation and expanding the interpretation of criminal law in judicial practice.[491] This view has particular practical significance. It shows that in the face of changes in the criminal situation caused by advances in science and technology, a relatively radical attitude and method is adopted to realize the social security function of criminal law. Online obscene live streaming, at its root, is a cybercrime. The attitude of criminal justice to it, to a certain extent, reflects the attitude towards cybercrime.

In the context of China, the development of new judicial interpretations can be seen as New Legislation. Under the above premise, the New Interpretation should be an extensive explanation of criminal law in the judicial practice mentioned above. From a future perspective, the new legislation is, of course, the best way to solve problems in judicial

[491] See. BOHAO CAI, 2016; JIE MEI, 2017; YUNXIA PANG AND LI SUN, 2018; YUN TENG, 2018; GONGZHENG WANG, 2018; MOLIN ZHAO: *The Legal Regulations on the Webcast* [网络直播的法律规制]. Changchun, China, Jilin University, 2017.

practice. If we only insist on this point in general, then the proposition, New Legislation or New Interpretation, proposed in this section has no practical significance. Therefore, the strategic choice of New Legislation or New Interpretation discussed in this section should be either the extensive explanation of contemporary criminal law by legal practice to achieve the requirements of crime control or crime prevention or follow the Principle of Legality in criminal law strictly with tolerant and prudent attitude to relevant crimes with the view of fulfilling the functions of human rights protection of criminal law before the enactment of New Legislation. This section prongs to stand by choice of New Legislation.

Criminal law is always chasing the crime. As for crime, it does subject to many factors of society, such as the development of technology. Cybercrime is a product of the emergence of ICTs, so is online obscene live streaming. Unduly restraint might arguably restrict the development of technology itself. For example, in the case of online live streaming, China has enacted many rules governing the online live streaming industry. There is a regulation in the Provisions on the Administration of Internet Live-Streaming Services requiring the live streaming service providers to back up all the materials at their platform within at least 60 days to facilitate the investigation if some crimes are reported platform. In addition, there is a good question about who should pay the costs of any higher burdens imposed. In a UK case[492] that refers to the online infringement of copyrights, the court held the view that "[it] considered it perfectly reasonable for ISPs to pay the costs associated with blocking access to sites where infringing content has been made available." The court also held the viewpoint that "[t]he ISPs profit form services that the operators of the relevant Web sites use to infringe the Intellectual Property rights concerned, and the costs of implementing any order by it to block access could be regarded as an average overhead of carrying on ISP's business."[493] In China, enterprises should bear the cost by themselves. Some companies with a small-scale platform could not meet the requirement for lack of technologies or money, and they will be excluded from the market. Only some big companies with a big-scale platform that have abundant money and sophisticated technologies could be left in the market. As time passes, a monopoly is generated. So, when dealing with cybercrime, the development of technology and the improvement of the relevant industry should be taken into account with a tolerant and prudent attitude.

[492] *Cartier Int'l AG & Others v. British Sky Broadcasting Ltd & Others*, EWCA Civ 658 [2016].

[493] GILL GRASSIE: The Campaign Against Hate Crime Online-Can Lessons be Learned from the IP Takedown Experience to Date? *Journal of Internet Law*, vol. 21. no. 5. (2017) 3-9.

Furthermore, the realization of human rights protection through strict adherence to the Principle of Legality in criminal law is an essential component of the rule of law. Though the criminal policy of coping with online obscene live streaming instructed by the SHDF National Office through the "CleanNet 2019" campaign demands harsh crackdown, it should subject the investigation, prosecution, and adjudication to the principle of legality, as *Lisztshe Trennung*, conceptualized by Claux Roxin, depicted that "*Das Strafrecht ist die unübersetzbare Schranke der Kriminalpolitik* (Criminal law is the untranslatable barrier of criminal policy)."[494] It could also be understandable, in other words, that the Principle of Legality in criminal law is the untranslatable barrier of criminal policy. Although Prof. Roxin had criticized it, the Lisztshe Trennung still has its value of preventing criminal policy overriding the principle of legality of criminal law, especially in the context of coping with cybercrime. In short, adhering to the Principle of Legality in criminal law is helpful to the judicial practitioners in the popularity of criminal law superstition stay awake. It is not conservative but virtue of tolerance and prudence.

2.4 STAGED SUMMARY

The unique feature of against the obscenity with a broad and sweeping attitude in China has made more distinction of coping with or dealing with online obscenity or pornography from other countries around the world. The new form of disseminating obscenity online, the online obscene live streaming with particular features itself or of the perpetrators and users involved, attracted more attention from the SHDF National Office in China and was treated as the primary target of the "CleanNet 2019" campaign. Cases reported by the SHDF National Office have shown the Chinese legal practice of the criminal justice system in coping with or dealing with online obscene live streaming. The governance of online obscene live streaming, at its root, is a type of cybercrime governance. By comparing with some analogical cybercrime researches about sexting and case study of the five example cases, general and particular problems had been selectively identified. Due to the particular situation of China, the feasible solutions, which are not only for the crime of online obscene live streaming but also other cybercrime under similar circumstances, call for different strategic choices: *Explanation Extension of Current Legislation*. With full consideration of the principle of legality (both in *legal dogmatic*s of criminal law and dialectic relationship between criminal law and criminal policy) and the prudence and

[494] See. CLAUS ROXIN: *Kriminalpolitik und Strafrechtssystem. 2. um ein Nachw. erw*. Aufl Berlin/Boston, De Gruyter, 1973.

tolerance underlying the criminal law, this section stands by choice of *Explanation Extension of Current Legislation* which requires to follow the Principle of Legality in criminal law strictly with tolerant and prudent attitude to relevant cybercrimes with the view of fulfilling the functions of human rights protection of criminal law.

Lessons should be learned from the practice of online obscene live streaming governance in China that: The development of information technology has prompted the emergence of some new types of crimes. Rather than a new type of crime, it is better to say that traditional crime presents unique characteristics. These so-called new crimes are constantly challenging the existing legal system. In other words, the current legal and regulatory system has shown a certain degree of lag and weakness in responding to new criminal situations. However, the increasingly new severe cybercrime has forced the official to respond to explanation extensions based on the existing legal system. Explanation extensions are trying to find a fulcrum between existing legal norms and new types of cybercrime. The principle of legality crimes must be followed to find this fulcrum in cybercrime governance. Generally speaking, it allows the official to interpret and expand the current legal norms, but the limit is that it cannot break through the principle of legality. Although the explanation extensions embodied in China's practice of online obscene live-streaming crime governance is debatable in terms of whether it breaks through the principle of legality, in general, it is within a certain reasonable range while maintaining a tolerant and cautious attitude.

3. Economic Innovation Protection and Cybercrime Governance: Online Platform Operator's Culpable Possibility in the Internet Sharing Economy

3.1 Internet Sharing Economy and Its Application

The *sharing economy* has been a pretty hot topic recently in China. However, sharing economy is not a new subject. It comes from the term "Collaborative Consumption," which Marcus Felson and Joe L. Spaeth promoted.[495] The sharing economy can also be called a collaborative economy, peer-to-peer economy, and access economy. It is "a mode of consumption whereby goods and services are not owned by a single user, but rather only temporarily accessed by members of a network and underutilized assets are shared, either for

[495] MARCUS FELSON AND JOE L. SPAETH: Community Structure and Collaborative Consumption: "A Routine Activity Approach". *The American Behavioral Scientist*, vol. 21. no. 4. (1978) 614-624.

free or for a fee."[496]

Nowadays, the sharing economy has shaped modern lives in many aspects. With the application of information communication technologies, the sharing economy has had a new form of Internet sharing economy and flourished more than before thereof. The Internet sharing economy can be traced in many areas, such as carpooling, peer-to-peer banking, Airbnb, and so forth. The Internet sharing economy consists of three parts: (a) redistribution markets, such as Swap-trading; (b) collaborative lifestyles, such as Land share; (c) the product-service system, which is the most popular and common now. Many Internet sharing economy products or services are included in this type, such as carpooling.[497]

Then, according to part (c), which arguably predominates the main characteristics of the sharing economy recently, the online platform appears. More and more new companies focus on the sharing economy. They may major in the different parts, such as the sharing vehicles like Drive My Car, the sharing real estate like Airbnb, and so on. All these new kinds of services have a common trait which somehow contains the Internet. They don't offer the goods or services the customers need directly but build a platform that permits the providers and the customers to match each other. Those platforms exist as an online form with a webpage or smartphone apps. Therefore, this section suggests calling them *online platforms*.

When they launch their business with the relevant web pages or apps, these companies might commit a crime or some crimes. For example, these companies abuse the clients' data offered for registration, intrude the personal privacy or violate some regulations or acts then commit a crime. I suggest claiming these circumstances the *culpable possibility*. Some of them could be avoided by prudence and loyalty, some of them might infeasibly be evaded under the development of technologies, or some of them are caused by the irrational regulations coded in the criminal law.

As discussed previously, this subsection provides definitions for several key terms used throughout this section, including Internet Sharing Economy, Online Platform, and Culpable Possibility. The following writings will primarily focus on the carpooling or ride-sharing services backup by the Internet sharing economy. This section will demonstrate the

---

[496] THE INVESTOPEDIA TEAM: *Sharing economy*. Investopedia, 1 April 2019, https://www.investopedia.com/terms/s/sharing-economy.asp

[497] RACHEL BOTSMAN: *The case for collaborative consumption*. TED, 1 April 2019, https://www.ted.com/talks/rachel_botsman_the_case_for_collaborative_consumption

DiDi hitch service. Analyze criminal cases involving this service and discuss its culpability in China. Additionally, this section will discuss the role that criminal law should play in light of the need for the development of new area technologies and the protection of new forms of economy.

3.2 DiDi Cases in China

3.2.1 Didi Chuxing

"Didi Chuxing (after this, DiDi) is the company in China which offers a full range of app-based transportation options for 550 million users, including Taxi, Express, Premier, Luxe, Bus, Designated Driving, Enterprise Solutions, Bike Sharing, E-bike Sharing, Car Sharing, and food delivery. Over 31 million drivers have found flexible work and income opportunities on the DiDi platform." [498] In 2015, DiDi, and KuaiDi, another online transportation service platform in China that had once been the rival of DiDi before, tied up.[499] In 2016, DiDi merged with Uber China.[500] After that, Didi has obtained a monopoly position in the carpooling service of online platform providers in China.

In June 2015, DiDi started to launch a new business that is DiDi Hitch Service. The DiDi hitch service, in other words, is the ride-sharing or carpooling service. The ordinary car owner, who is not the particular driver engaged in the DiDi Express or Premier or Luxe service, could release some information about his/her routine to seek an accompany who has the same destination with the driver or has a large ratio of their respective routine. The customer should pay the fees to the driver for the sharing. In general, the money they pay for the ride-sharing service is much less than taking a taxi within the same distance. So, at first, it attracted many users to try this new method of transportation. On the other hand, the driver can get paid back to compensate his/her general cost of the car. It's a win-win innovation.

However, such a convenient service was suspended in August 2018 for compulsory business adjustment. Not only that, but Didi also faces criminal risks, or some scholars believe it should be criminally responsible for its security issues. Its users have criticized the security problems of the DiDi hitch service. Many passengers, most of whom are female, complained about sexual harassment or sexual invasion.

---

[498] DIDI: *About us*. DiDi. Inc, 1 April 2019, https://www.didiglobal.com/about-didi/about-us

[499] GERRY SHIH: *China taxi apps Didi Dache and Kuaidi Dache announce $6 billion tie-up*. Reuters, 1 April 2019, https://www.reuters.com/article/us-china-taxi-merger-idUSKBN0LI04420150214

[500] EMILY RAUHALA: *Uber loses bid for China business, plans to merge with main rival*. The Washington Post, 1 April 2019, https://www.ndtv.com/world-news/uber-loses-bid-for-china-business-plans-to-merge-with-main-rival-1438797

3.2.2 Fifty Sample Criminal Cases of DiDi

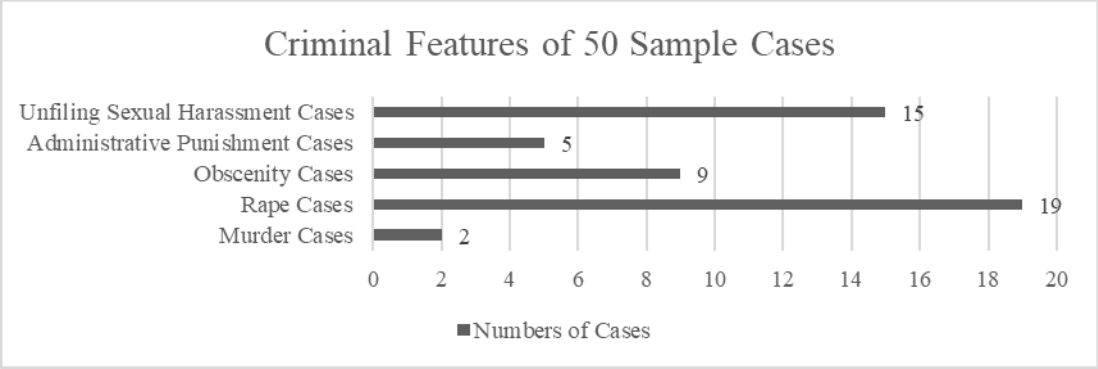

Figure IV. 3.2-1 Criminal Features of 50 Sample Cases Related to DIDI

A report was given by the journalists of infzm.com, which is based on 50 sexual harassment or invasion cases as samples related to the DiDi hitch drivers. The judgment could be downloaded from the open accessed database of the judicial court in different areas in China. These 50 sample cases happened from May 2015 to May 2018, in 4 years. The age of the 50 suspects varied from 22 years old to 40 years old. The age of the 53 victims involved varied from 16 years old to 31 years old. According to the announced education level of 10 suspects in 50 suspects, three drivers of the ten are at the middle school level, seven drivers of the ten are at the high school level. The author also analyzed the nature of the 50 cases, see Figure IV. 3.2-1.[501]

Two cases related to the DiDi hitch service had gone viral on social media and attracted much attention for introspecting the security issues during the service providing.

The first happened on 6 May 2018. The victim was a 21-year-old flight attendant. She ordered a ride on DiDi hitch service after works. However, she was raped and murdered by the driver, which she matched on the DiDi platform. The suspect was a 27-year-old male. Depending on the investigation from the police, the suspect stole his father's ID and some other information to complete a fake registration, and he also passed the facial recognition system of the DiDi.[502]

Chinese netizens and Didi users expressed intense anger on the one hand. On the other hand, this matter also made people pay attention to the safety of services and the follow-up repair methods of Didi. Then, DiDi suspended this service for a period, updated the

[501] HUANHUAN LUO: *50 Sexual Invasion Sample Cases and "Didi Rectification"* [50 个性侵犯样本与滴滴整改], infzm.com, 1 April 2019, http://www.infzm.com/contents/136003

[502] YI ZHANG AND XIN QI: *Didi suspends 'hitch' service after driver allegedly kills passenger*. China Daily, 1 April 2019, http://www.chinadaily.com.cn/a/201805/12/WS5af62b55a3103f6866ee7ec5.html

safety system, and improved the hitch service driver threshold.[503]

However, just after three months of this rectification, in August 2018, there was another felony offense against the passenger during the ride-sharing. On 24 August 2018, in Wenzhou in China, a 20-year-old woman was raped and murdered by the driver of the DiDi hitch service, which she ordered on the DiDi platform. This incident had some similarities with the one that happened in May 2018, but what made the Chinese people feel so angry with DiDi was that, before the victim lost contact, she tried to ask for help from DiDi customer service. The negative attitude and bureaucratic measures of the DiDi customer service made the victim lose the best timing and chance to immune from this 'nightmare.' The victim also sought help from her friends, and the chatting history recorded the whole process of asking emergency help from DiDi.

Just in three months, two female passengers were raped and killed during the hitch service. In this period, DiDi claimed to update their system to secure safety. But the results were the opposite. The users of DiDi criticized its attitude and measures fiercely on the Internet. The government of China also made some commands to force the DiDi to suspend this service and do the rectifications.[504]

3.3 Culpable Possibility and Online Platform Operators

3.3.1 Doctrine of Article 286(I): A Source of Culpability

According to the cases introduced above, it could easily find that the felony offenses against the passengers during the hitch service were not rare but arguably common within the DiDi hitch service online platform. There is no doubt that the suspect drivers in these cases should be punished under criminal law. However, under the circumstance of DiDi updating the security system and being complained about by the users many times, should DiDi bear the criminal liability in similar cases? Furthermore, should some online platforms of sharing economy like DiDi hitch assume criminal liability when users experience infringement of their rights protected by the criminal law? If the answer was "Yes," then it means these platform providers, the company, should endure the criminal risk for providing the platform and in their management process.

Chinese criminal law offers the possibility and feasibility to criminalize the relevant

[503] BBC NEWS: *China car app Didi updates safety measures after murder*. BBC, 1 April 2019, https://www.bbc.com/news/technology-44143297

[504] BBC NEWS: *Didi Chuxing suspends carpool service after woman killed*. BBC, 1 April 2019, https://www.bbc.com/news/world-asia-china-45313074

conduct with the *mens rea* of knowingly, negligence, and reckless, or punish the natural person or legal person who fails to perform the management obligation of information network security, and refuses to make correction measures after being ordered by the regulatory authority to take corrective actions, then causes the serious circumstance happened.[505] Now, we date back to the DiDi cases we mentioned above. The DiDi company or the hitch service department of DiDi fails to supervise the drivers well to cause some persons with malicious purposes to be hitch service drivers. The threshold of being a hitch service driver is lower than being a particular driver for the other DiDi transportation service, such as Express, Premier, and Luxury. It means that DiDi has two admittance standards. One is rigorous, and the other one is relatively loose.

On the one hand, due to the distinguish of the admittance standards, these drivers with loose supervision caused fatal offenses to the passengers. Many passengers treated all the drivers on the DiDi platform as the particular driver with the strict standard and didn't know the difference between the specific DiDi driver and hitch service driver. On the other hand, the passenger chose the DiDi hitch service as the means of transportation because of the lower price with the same distance, which is out of the trust to the DiDi platform. DiDi's failure to supervise the hitch service drivers violated the principle of trust. Then, it could be a negligent offender in these cases.[506]

But, article 286(a) regulates another critical scenario, i.e., refusing to make corrections after being ordered by the regulatory authority to take corrective measures. Some scholars in China treated this requirement in the criminalization as a reasonable condition, thereby preventing the over-wide broader of this crime.[507] Then, here came the question of whether the DiDi has had this condition; in other words, refusing to make corrections. Some scholars hold the view that DiDi didn't refuse to make corrections. DiDi did some rectifications after the Zhengzhou incident in May 2018. After that case, DiDi made some rigorous conditions for the hitch service drivers. The case that happened in August could not

---

[505] See. Article 286(I) of the *Criminal Law of the Peope's Republic of China* (For more details about this offense, please see Chapter II-2.2 & Chapter III-4.1)

[506] See. WEI YOU AND XIMEI XIE: The Principle of Trust and Its Application in the Negligent Crimes [信赖原则及其在过失犯罪中的运用]. *Science of Law (Journal of Northwest University of Political Science and Law)* [法律科学(西北政法大学学报)], no. 5. (2001) 56-65.

[507] See. ZIYANG LI: The Obligation Stereotype and the Criminal Liability Determination of the Hitch Service Online Platform: Thoughts Caused by Zhengzhou Flight Attendant Case and Wenzhou Preschool Teacher Case [顺风车网络平台的义务定型及刑事责任认定：由郑州空姐案、温州幼师案引发的思考]. *Journal of Jiangxi Police Institute* [江西警察学院学报], no. 1. (2019) 60-66.

attribute to DiDi.

Furthermore, after the Wenzhou incident in August 2018, DiDi had already shut down the hitch service. Ten government ministries in China had already sent officials to DiDi to supervise rectifying the hitch service. So, the attitude of DiDi is positive. It cannot be blamed too much for protecting the new form of sharing economy and encouraging the innovation of online technologies.[508]

3.3.2 Is DiDi Culpable? China's Handling

This section held that DiDi had a condition that refused to make corrections.

First, these two cases were not the only two cases that happened before. As introduced before, there were at least more than 50 cases. Before the first time, DiDi suspended the hitch service and rectified it in May 2018; many females were suffering sexual harassment and invasions. DiDi responded too late to cause the new crimes that happened once more.

Second, the effectiveness and efficiency of the rectification should be considered under the condition of refusing to make corrections after being ordered by the regulatory authority to take corrective measures in Article 286(I). To justify whether the service providers positively make corrections, on the one hand, is to investigate if they do the rectifications; on the other hand, it is to evaluate if they do the corrections right, i.e., effective and efficient. It has reasonable reasons to believe that if the DiDi took efficient and effective tinkering to its security system, there would not be any similar fatal incidents that happened so frequently, at least, in three months, from May to August.

So, this section believes that DiDi didn't take a positive approach that refuses to make corrections directly rather than a negative method, making some ineffective and inefficient corrections. Didi's approach and attitude has further led to a large number of criminal cases. Therefore, Didi should be culpable and should be found to constitute a crime under article 286(I) of the Criminal Law, i.e., *Crime of Refusing to Fulfill the Obligation of Information Network Security Administration*.

Although DiDi should bear criminal liability, at least in the Wenzhou case, the government of China didn't put DiDi into the criminal justice. There was a saying from the report released by the Sharing Economy Research Center under the State Information Center

[508] JIANFENG YIN: *The component of the requirement of refusing to make corrections under the article 286(a) of Criminal Law of China*, 25 March 2019. [A Private Conversation with Prof. Yin Jianfeng from Law School of Beijing Normal University on Understanding of Article 286(a) of Criminal Law of China.]

that, which might represent the policy of China to the online platform of sharing economy, "rules will be formulated for emerging industries with the principle of encouraging innovation and conducting regulation in a tolerant and prudent way."[509]

Nonetheless, it is necessary to discuss culpable possibility. While the DiDi was granted forgiveness this time, this does not mean that all of these incidents are immune from criminal liability. As long as article 286(I) remains operational, there is a chance that the DiDi will bear criminal liability. DiDi is not the sole provider of online sharing economy platforms. This means that all sharing economy platform providers face a culpable possibility, at least in China.

Culpable possibility appears to be a negative concept. However, a careful examination of the internal logic reveals a double-edged sword. On the one hand, because culpable possibility exists, enterprises that provide online platforms for the sharing economy will invest heavily in prudently implementing active and effective supervision in order to avoid criminal liability to the greatest extent possible. On the other hand, suppose allowing these businesses to develop freely, and they are immune from criminal prosecution. In the case of DiDi, users will cease using related products for security reasons, effectively ending their participation in Internet sharing economy. Businesses will face the prospect of closure. That is not what we are anticipating. Thus, to a degree, appropriate culpable possibility is beneficial to the long-term development of providers of sharing economy online platforms.

A balance must be stroke between safeguarding economic innovation and new economic forms and ensuring the fundamental rights of users. Approaching the sharing economy's negative consequences with caution and tolerance is important. This does not mean, however, that cybercrime governance should abandon criminal control of Internet sharing economy. A proportionate increase in the culpable possibility faced by providers of shared economic online platforms should become a global trend. Using "culpable possibility" to instill a sense of security in the user is a rational strategy. Cybercrime governance should impose strict limits on the appropriate boundaries of this strategy, while it cannot abandon this strategy's adoption.

3.4 STAGED SUMMARY

At first glance, the Didi case discussed in this section seems to have little to do with

[509] XINHUA NEWS: *China's "sharing economy" up 103 pct in 2016: Report*. Xinhua Net, 1 April 2019, http://www.xinhuanet.com//english/2017-03/05/c_136104460.htm

cybercrime governance. However, Chapter II offered a generalized definition of cybercrime and discussed the morphology of cybercrime, respectively. Whether it is based on the general definition of cybercrime given in this dissertation, or according to the morphology of specific cybercrime in Chinese criminal law, the *Crime of Refusing to Fulfill the Obligation of Information Network Security Administration* should belong to the category of cybercrime. Secondly, this section also discusses the culpable possibility of online platform operators. Whether online platform operators, such as DiDi discussed in this section, should bear criminal liability under certain circumstances is of course within the scope of cybercrime governance.

It has been nearly 30 years since the Internet became widespread for both commercial and civilian use. The Internet economy has constantly innovated, from the former two-way relationship between Internet enterprises and users to the triangle relationship "users-online platform operators-users." The Internet sharing economy is also a form of expression of this triangle. Recognizing the possibility of criminal liability of online platform operators represents a new logic of cybercrime governance and an ideological development of cybercrime governance.

The culpable possibility of the Hitch Service platform provider discussed in this section is indeed the relationship between cybercrime governance and the encouragement of new economic forms and new technological development. In other words, in the context of the continuous development of the Internet economy and the continuous progress of information network technology, what kind of attitude should the authorities maintain to carry out cybercrime governance?

In this part of the discussion, it is believed that according to the current provisions of China's Criminal Law [Article 286 (I)], DiDi Company should be culpable for cybercrime on its operating platform caused by management negligence. However, China's practice suggests a relatively "tolerant" attitude towards DiDi. The Chinese government has not taken DiDi to criminal court for the cases described above. It is a choice made by the Chinese government after fully considering the country's "Internet+" policy and the development trend of the Internet sharing economy.

Lessons should be learned from the DiDi cases in China that we should not blindly pursue cybercrime governance without considering the background of social and economic development and the progress of information network technology. Social progress and

development are made up of progress in all aspects, and progress in crime control is only part of the overall social development. It is unwise to realize cybercrime governance at the expense of technological progress and economic development. We should not blindly believe in the role of criminal law in cybercrime governance. At the same time, not fetishizing criminal law does not mean abandoning Criminal Law methods to engage in cybercrime governance. In the process of cybercrime governance, criminal law should be moderately tolerant and cautious about responding to people's demand for crime governance and ensuring technological progress and economic development.

V. AN ANALYSIS OF SENTENCING DISPARITY AND AUXILIARY CYBERCRIME: THE SENTENCING PRACTICE

Sentencing Disparity of Auxiliary Cybercrime in Criminal Justice in China[510]

Conviction and sentencing are two essential steps that cannot be avoided in criminal justice. The previous chapter mainly discusses the practice and experience of how to formulate and apply policies and laws, especially criminal policies and criminal laws, in cybercrime governance in China, namely, the conviction of cybercrime. Different from the previous chapter, this chapter mainly discusses the practice and lessons of sentencing cybercrime in Criminal justice in China. To some extent, the fairness of sentencing reflects the level of cybercrime governance. This chapter focuses on the sentencing disparity of the two types of cybercrimes by taking the sentencing practice of them stipulated in the Amendment IX of Criminal Law of China as the research object. In terms of research methods and structure, this chapter is quite different from the previous chapters. This chapter mainly adopts the method of empirical analysis and adopts the general structure of empirical research. Here comes this chapter.

1. OVERVIEW

The sentencing disparity is a thesis that is not new but consistently researched with great academic passion in criminology, criminal justice, or even criminal law research. It comes from the concern with how the sentences are determined and whether perpetrators under relatively similar circumstances receive similar sentence outcomes.[511] Notably, there is an endogenous value conflict in the sentencing decisions from where the sentencing outcomes to individual perpetrators come between "goals of equal justice under the law and individualized justice with punishment tailored to the offender."[512] The latter value orientation is based on the theoretical paradigm of rehabilitation. The offenders could have the chance to return to society with some corrections, not just the penalties in prison. Judges

[510] This chapter mainly draws on my article published in *Iustum Aequum Salutare*: *Sentencing Disparity in China: A Descriptive Research on Auxiliary Cybercrime Stipulated by Amendment IX of Criminal Law*. See. DAWEI SONG: Sentencing Disparity in China: A descriptive Research on Auxiliary Cybercrime Stipulated by Amendment IX of criminal law. *Iustum Aequum Salutare*, vol. XVII. no. 2. (2021) 209-239.

[511] PATRICIA L. BRANTINGHAM: Sentencing disparity: An analysis of judicial consistency. *Journal of Quantitative Criminology*, vol. 1. no. 3. (1985) 281-305.

[512] BARBARA A. KOONS-WITT: Equal justice versus individualized justice: Discretion and the current state of sentencing guidelines. *Criminology & Public Policy*, vol. 8. no. 2. (2009) 279-283.

were expected to mete out individualized sentencing to a particular offender according to their specific characteristics.[513] However, there was a reform movement of sentencing in the United States by criticizing rehabilitation, especially the failure to reduce recidivism.[514] The reform was intended to constrain the discretion, which is the direct causation of judges' disparity when sentencing the offenders. "It shifted the prime foci of corrections from rehabilitation to retributions and deterrence, which made responses to crime more severe and tangible." [515] Then, it seems that sentencing reform aims to get similar sentencing outcomes within similar cases under uniform sentencing guidelines, for instance, the Federal Organizational Sentencing Guidelines in the United States. Meanwhile, this kind of goal and practices leave room for the academic discussion of sentencing disparity.

When researching the sentencing disparity, there is a core question that could not be avoided: what factors should be considered in sentencing? Brantingham exemplified the questions about whether case facts, personal background, and the potential for recidivism should be considered in the process of sentencing.[516] On the premises of these questions, the later researchers, in general, classified the factors into two types: legal relevant factors, such as crime seriousness, criminal career status, acceptance of the guilty; and extralegal factors, such as age, gender, education, employed status, race/ethics, et cetera.[517] It is easy to

[513] RONALD S. EVERETT AND ROGER A. WOJTKIEWICZ: Difference, Disparity, and Race/Ethnic Bias in Federal Sentencing. *Journal of Quantitative Criminology*, vol. 18. no. 2. (2002) 189-211.

[514] ROBERT MARTINSON: What works-questions and answers about prison reform. *Forensic Quarterly*, vol. 50. no. 2. (1976) 225-248.

[515] NORVAL MORRIS AND MICHAEL TONRY: Between prison and probation: Intermediate punishments in a rational sentencing system. Oxford University Press, 1991.

[516] PATRICIA L. BRANTINGHAM, 1985, pp. 284-285.

[517] e.g., PATRICIA L. BRANTINGHAM, 1985, pp. 284-285; RONALD S. EVERETT AND ROGER A. WOJTKIEWICZ, 2002, pp. 196-209.; MARVIN D. FREE: Racial Bias and the American Criminal Justice System: Race and Presentencing Revisited. *Critical Criminology*, vol. 10. no. 3. (2001) 195-223; REBECCA L. LOEFFLER AND TIMOTHY J. LAWSON: Age and Occupational Status of Defendant in relation to Mock Juror Sentencing Recommendations. *Current Psychology*, vol. 21. no. 3. (2002) 289; DARRELL STEFFENSMEIER AND STEPHEN DEMUTH: Does Gender Modify the Effects of Race–ethnicity on Criminal Sanctioning? Sentences for Male and Female White, Black, and Hispanic Defendants. *Journal of Quantitative Criminology*, vol. 22. no. 3. (2006) 241-261; JEFFERY T. ULMER, JAMES EISENSTEIN AND BRIAN D. JOHNSON: Trial Penalties in Federal Sentencing: Extra-Guidelines Factors and District Variation. *Justice Quarterly*, vol. 27. no. 4. (2009) 560-592; FRANK MCINTYRE AND SHIMA BARADARAN: Race, Prediction, and Pretrial Detention. *Journal of Empirical Legal Studies*, vol. 10. no. 4. (2013) 741-770; TARA N. RICHARDS, M. DWAYNE SMITH, WESLEY G. JENNINGS, BETH BJERREGAARD AND SONDRA J. FOGEL: An Examination of Defendant Sex Disparity in Capital Sentencing: A Propensity Score Matching Approach. *American Journal of Criminal Justice*, vol. 39. no. 4. (2014) 681-697; TRACI BURCH: Skin Color and the Criminal Justice System: Beyond Black-White Disparities in Sentencing. *Journal of Empirical Legal Studies*, vol. 12. no. 3. (2015) 395-420; RHYS

understand the legally relevant factors that would impact the sentencing outcomes because, generally, most of the legally relevant factors have been ensured by or coded in the sentencing guidelines. However, the research mentioned above seems to pay more attention to the extralegal factors that could influence the sentencing. There is an inner logic presupposition that these researchers prefer to the sentencing uniformity. Under this premise, researchers expect to find the departure or failure of the sentencing guidelines in the process of sentencing by examining the significant impact of the extralegal factors in sentencing.

Coincidently, China also has a sentencing guideline for instructing the sentencing process during the trial. In the Sentencing Guideline for Common Crimes, which was promulgated by the Supreme People's Court of China, sentencing uniformity is basic.[518] With the principle in the Chinese judicial practice, the current study is endowed the research meaning to discuss the sentencing disparity in China's contextual environment. However, compared with the abundant research on the sentencing disparity in the United States and European countries, quantitatively, the relevant research or sentencing disparity studies are relatively less in Chinese scientific literature. On the other hand, due to the present researches as to sentencing disparity in China, they had different foci, for example, the disparity in the traffic crimes[519], the application of probation[520], the regional disparity of bribery crime[521], the

---

HESTER AND TODD K. HARTMAN: Conditional Race Disparities in Criminal Sentencing: A Test of the Liberation Hypothesis from a Non-Guidelines State. *Journal of Quantitative Criminology*, vol. 33. no. 1. (2017) 77-100; JOHN M. MACDONALD AND ELLEN A. DONNELLY: Evaluating the Role of Race in Sentencing: An Entropy Weighting Analysis. *Justice Quarterly*, vol. 36. no. 4. (2017) 656-681; BYUNGBAE KIM, XIA WANG AND HYUNJUNG CHEON: Examining the Impact of Ecological Contexts on Gender Disparity in Federal Sentencing. *Justice Quarterly*, vol. 36. no. 3. (2018) 466-502; KELSEY L. KRAMER AND XIA WANG: Assessing Cumulative Disadvantage against Minority Female Defendants in State Courts. *Justice Quarterly*, vol. 36. no. 7. (2019) 1284-1313; NOAH PAINTER-DAVIS AND JEFFERY T. ULMER: Discretion and Disparity under Sentencing Guidelines Revisited: The Interrelationship between Structured Sentencing Alternatives and Guideline Decision-making. *Journal of Research in Crime and Delinquency*, Published online (2019)

[518] SUPREME PEOPLE'S COURT: *Sentencing Guideline for Common Crimes Supreme People's Court*, 31 July 2014, http://www.court.gov.cn/shenpan-xiangqing-6622.html

[519] e.g., YANYU XIN AND TIANJI CAI: Paying money for freedom: Effects of monetary compensation on sentencing for criminal traffic offenses in China. *Journal of Quantitative Criminology*, Published online, (2019)

[520] e.g., XINGHONG ZHAO: The Application of Probation in China: An Empirical Study Using Chinese Judicial Documents [缓刑适用的中国图景：基于裁判文书大数据的实证研究]. *Contemporary Law Review* [当代法学], vol. 31. no. 2. (2017) 46-61.

[521] e.g., JIANBO WANG: An Empirical Research on Regional Disparity of Bribery Crime Sentencing in China [我国受贿罪量刑地区差异问题实证研究]. *China Legal Science* [中国法学], no. 4. (2016) 245-265.

sentencing outcomes of gender disparity in violent offenses[522], and general research of the disparity from a macro-level perspective [523]. However, the existing research on the sentencing disparity in China rarely considers the sentencing disparity in cybercrime, which is the most "prevalent" crime related to information technologies worldwide and attracts more attention in criminology criminal justice scholarship. On the premise, to fill the gap, the current research purports to explore the influence of both legally relevant factors and extralegal factors extract from the real cases have on the sentencing outcomes for auxiliary cybercrime according to Article 287(I) and Article 287(II) of Chinese Criminal Law which amended by the Amendment IX of Criminal Law.

Auxiliary cybercrime is not a criminological terminology but summarized by the current research. To identify the auxiliary cybercrime, it is worthy of figuring out the concept of cybercrime first. Cybercrime is not a concept of criminal law within legal dogmatic but a criminological terminology.[524] The current research applied the concept of cybercrime that cybercrime is conducted utilizing the Internet or ICTs to endanger society and jeopardize citizens' legal rights and interests or attack and destruct the computer system.[525] Cybercrime relies on an information network technology to gradually penetrate traditional crime and combine it to present new characteristics. Criminal lawmakers, criminal law practitioners, and criminal law researchers have reached a consensus that the current criminal legislation can no longer keep up with the pace of cybercrime mutation. Under the influence of the Risk Society Theory, to adequately cope with and control cybercrime development, full process monitoring, and early law enforcement intervention have become the preferred criminal legislation choices.[526] With this perspective, by the instruction of related criminal policy,

---

[522] HONG LU, BIN LIANG AND SIYU LIU: Serious Violent Offenses and Sentencing Decisions in China—Are There Any Gender Disparities? *Asian Journal of Criminology*, vol. 8. no. 3. (2013) 159-177.

[523] e.g., see. JIANJUN BAI: *Empirical Criminal Law and Sentencing Practice: Big Sample Perspective on Criminal Law Phenomena* [刑法规律与量刑实践：刑法现象的大样本考察]. Beijing, Peking University Press, 2011; JOHN ZHUANG LIU AND XUEYAO LI: Legal Techniques for Rationalizing Biased Judicial Decisions: Evidence from Experiments with Real Judges. *Journal of Empirical Legal Studies*, vol. 16. no. 3. (2019) 630-670.

[524] DAWEI SONG: What is Cybercrime? A criminology Perspective. *Public Goods and Governance*, vol. 3. no. 2. (2018) 10-15.

[525] CHINA JUSTICE BIG DATA ACADEMY: *Features and Trends of Cybercrime (2016.1-2018.12)*. China Justice Big Data Service Platform, 19 November 2019, https://pdfs.semanticscholar.org/ee29/6776064640534a9041f5856051b15fd6ef76.pdf

[526] JIANPING LU: Criminal Policy and Criminal Law in the Risky Society [风险社会的刑事政策与刑法]. *Legal Forum* [法学论坛], vol. 26. no. 4. (2011) 21-25; SUPREME PEOPLE'S COURT: *Press conference on the 'Interpretations of the supreme people's court and supreme people's procuratorate on the application*

Chinese criminal legislators labeled some preparatory and assistive behaviors in committing a cybercrime as independent crimes within the criminal law. In 2015, China enacted the Amendment IX of Criminal Law. Two types of cybercrime have been stipulated in the penal code, i.e., Article 287(I), which criminalizes the illegal utilization of information network technology, and Article 287(II), which criminalizes the provision of assistance to conduct cyber-criminal activity. According to the traditional joint crime theory, the principals of these two clusters of conduct could not have been charged if the principals of the main crime had not been convicted, but, now, the accomplice conduct can be judged separately from the cybercrime. In other words, the offenders could be convicted regardless of whether the other perpetrators of the related main crime were charged. Furthermore, due to these conduct's endogenous assistive characteristics in the two articles, the current research summarizes them as auxiliary cybercrime.

This study aims to untangle why the sentencing disparity should be researched with sampling from the auxiliary cybercrime. The reasons for or meaning of the current research could attribute to the following aspects. First, the amount of sentencing disparity results of Chinese research is rarely compared with the US or European research results. The current research will fill the gap to some extent. Second, the current research aims to discover cybercrime's sentencing situation in China, which would arguably enrich cybercrime research. Third, because of the features of auxiliary cybercrime, including that the relatively new stipulations in the Chinese Criminal Law have just been four years implementations, from 2015 to 2019, the caseload is not very large, and the sampling could cover most of the real cases which is beneficial to find the analytical results. As an official of the Supreme People's Court reported, from 2015 to September 2019, the aggregated number of both cases was 260 and covered 473 offenders.[527] Lastly, the Supreme People's Court and Supreme People's Procuratorate have enacted a new judicial interpretation of auxiliary cybercrime. This judicial interpretation could be the sentencing guideline of auxiliary cybercrime in the future. However, all the cases sampled in the current are those judgments before it. So, on the one hand, the current research aims to discover the sentencing disparity of auxiliary cybercrime and find the salient factors that could influence the sentencing outcomes; on the

of laws in handling criminal cases of illegal utilizing information network technology and assisting cyber-criminal activities' [《最高人民法院、最高人民检察院关于办理非法利用信息网络帮助信息网络、犯罪活动等刑事案件适用法律若干问题的解释》新闻发布会], 25 October 2019, http://www.court.gov.cn/zixun-xiangqing-193671.html

[527] SUPREME PEOPLE'S COURT, 2019.

other hand, the current research could be treated as preliminary research for future research on the sentencing disparity of auxiliary cybercrime, especially on the comparison of the sentencing disparity before and after the judicial interpretation.

As mentioned above, the number of researches on the sentencing disparity in China is relatively rare compared with other countries' academy. When combining the sentencing disparity with cybercrime, the number of researches is less. The current research inclines to learn more from the relevant research in the United States, Canada, and European Countries. As a research model, the current research applies the research paradigm from Brantingham's work that classified the factors into four categories: case facts, offender characteristics, system operational factors, and judge characteristics.[528] As for the offender characteristics, scholars, especially in the United States, generally examined the race/ethnics influence on the sentencing outcomes.[529] However, the contextual environment is radically different between China and the United States. In China, race discrimination is not very significant. Instead, regional discrimination seems to have arguably much more influence in all processes of social operation.[530] The objectives, but not the whole, of the current study are trying to answer and give preliminary explanations to the following questions:

1. Does disparity exist in the auxiliary cybercrime sentencing outcomes in China?
2. How much of these disparities depend on the legally relevant factors, such as types of conduct, the seriousness of the crime, status in the crime, the convergence of other crimes, and joint/ unit crime?

---

[528] PATRICIA L. BRANTINGHAM, 1985, p. 285.

[529] e.g., RONALD S. EVERETT AND ROGER A. WOJTKIEWICZ, 2002, pp. 194-195; MARVIN D. FREE, 2001, pp. 199-219; DARRELL STEFFENSMEIER AND STEPHEN DEMUTH, 2006, p. 247; FRANK MCINTYRE AND SHIMA BARADARAN, 2013, pp. 743-747; ED A. MUNOZ AND ADRIENNE B. FRENG: Age, Racial/Ethnic Minority Status, Gender and Misdemeanor Sentencing. *Journal of Ethnicity in Criminal Justice*, vol. 5. no. 4. (2008) 29-57; JILL K. DOERNER AND STEPHEN DEMUTH: The Independent and Joint Effects of Race/Ethnicity, Gender, and Age on Sentencing Outcomes in U.S. Federal Courts. *Justice Quarterly*, vol. 27. no. 1. (2010) 1-27; ERIC P. BAUMER: Reassessing and Redirecting Research on Race and Sentencing. *Justice Quarterly*, vol. 30. no. 2. (2013) 231-261; XIA WANG AND DANIEL P. MEARS: Sentencing and State-Level Racial and Ethnic Contexts. *Law & Society Review*, vol. 49. no. 4. (2015) 883-915.

[530] e.g., see. GUOPING HUANG AND BENXIAN YAO: Regional Discrimination and the Construction of a Harmonious Society. *Science of Social Psychology*, vol. 21. no. 4. (2006) 50-52; SHUNYI LIU AND ZHENGCHUN LI: The Concentrated Effect of Regional Discrimination in China and the Construction of Anti-Discrimination System: Discussing the Vilification and Discrimination against Henan People [中国地域歧视的集中效应与反歧视体系建构：兼论丑化与歧视河南人现象]. *The Journal of Harbin Committee School of the CCP* [哈尔滨市委党校学报], vol. no. 4. (2010) 87-89.

3. Do these disparities depend on the offender's characteristics while controlling the legally relevant factors, such as age, gender, residence, educational level, and court location?

2. LITERATURE REVIEW

2.1 PRIOR RESEARCHES ON SENTENCING DISPARITY

There are two kinds of factors that could influence sentencing outcomes. The first is legally relevant factors that drew on the sentencing guidelines, and the second is extralegal factors, which are generally unmodified by the sentencing guidelines, including the offender's age, gender, race or ethnics, socioeconomic status. The research as to sentencing disparity could not steer clear of these two typical factors in their studies. The sentencing guidelines' function is to reduce the unwarranted disparity in sentencing; thus, it is understandable in most of the sentencing realities that the legally relevant factors have a significant impact on the sentencing outcomes. In other words, according to the Formal Legal Theory, the legally relevant factors should effectively predict the sentencing outcomes and could interpret "a greater magnitude of the variance than extralegal factors."[531] The research using the drug trafficking case data from the US Sentencing Commission from 1999 to 2002 of Kautt has proven this perspective.[532] However, in Kautt's research, the extralegal factors, age, gender, and race have explanatory effects. It is also the case with the bulk of sentencing disparity research that endeavors to describe, exploit, and explain the impact of extralegal factors on sentencing outcomes.

First of all, age influences shaping the sentencing outcomes. It arguably comes to a commonsense that there is more probability of younger offenders receiving harsher sentencing outcomes while, compared with older ones, sentencing is more lenient.[533]

---

[531] PAULA M. KAUTT: Is the Offense Serious Axis Free of Extralegal Influence? Assessing the Predictors of a 'Legally Relevant' Guideline Criterion. *American Journal of Criminal Justice*, vol. 34. no. 3. (2008) 253-273.

[532] PAULA M. KAUTT, 2008, pp. 253-273.

[533] e.g., ED A. MUNOZ AND ADRIENNE B. FRENG, 2008, pp. 48-49; DARRELL STEFFENSMEIER, JOHN KRAMER AND JEFFERY ULMER: Age Differences in Sentencing. *Justice Quarterly*, no. 3. (1995) 583-602; DARRELL STEFFENSMEIER, JEFFERY ULMER AND JOHN KRAMER: The Interaction of Race, Gender, and Age in Criminal Sentencing: The Punishment Cost of Being Young, Black, and Male. *Criminology*, vol. 36. no. 4. (1998) 763-798; BARBARA A. KOONS-WITT, ERIC L. SEVIGNY, JOHN D. BURROW AND RHYS HESTER: Gender and Sentencing Outcomes in South Carolina: Examining the Interactions with Race, Age, and Offense Type. *Criminal Justice Policy Review*, vol. 25. no. 3. (2014) 299-324; DARRELL STEFFENSMEIER, NOAH PAINTER-DAVIS AND JEFFERY ULMER: Intersectionality

Steffensmeier, Kramer, and Ulmer detailed the distinction among the different ranks of ages that young offenders, especially offenders within their 20s and early 30s, are more likely to get harsher sentences than those between 18-20, in their late 30s, and 40s or older.[534] Munoz and Freng found that, in misdemeanor sentencing, "young and young adults had a higher likelihood of receiving other punitive sentences, in addition to, or rather than just a fine."[535] When considering the interaction between age and other extralegal factors, Steffensmeier, Ulmer, and Kramer demonstrated that "age is more influential in male offenders' sentencing than female offenders."[536] Steffensmeier, Painter-Davis, and Ulmer combined gender and race with age and concluded that young black males received harsher punishment than those old defendants.[537] However, some researchers disagree with the proposition above and reach opposing results. For instance, in their studies on defendants' age and attractiveness, Smith, and Hed deduced those young or attractive offenders could get the sentencing outcomes with more leniency;[538] however, the old or unattractive offenders might get harsher sentences than therebefore.[539] Whether positive or negative impacts of age on sentencing, the reality is that age, as an extralegal factor, in most times, could influence the sentencing outcomes and cause the disparity.

The second extralegal factor with a heated discussion in the sentencing disparity research is gender. Due to this study's limited research resource, the research on gender disparity and sentencing results did not involve sexual minorities. Generally, researchers deploy a dichotomous classification of gender, that is, male and female. Most present studies show that female ones have a higher likelihood of receiving lenient sentencing outcomes compared with male offenders.[540] Some works did not show the inclination of favoring either

---

of Race, Ethnicity, Gender, and Age on Criminal Punishment. *Sociological Perspectives*, vol. 60. no. 4. (2017) 810-833.

[534] DARRELL STEFFENSMEIER, JOHN KRAMER AND JEFFERY ULMER, 1995, pp. 599-600.

[535] ED A. MUNOZ AND ADRIENNE B. FRENG, 2008, pp. 46-50.

[536] DARRELL STEFFENSMEIER, JOHN KRAMER AND JEFFERY ULMER, 1995, p. 599.

[537] DARRELL STEFFENSMEIER, NOAH PAINTER-DAVIS AND JEFFERY ULMER, 2017, p. 822.

[538] EDWARD D. SMITH AND ANITA HED: Effects of offenders' age and attractiveness on sentencing by mock juries. *Psychological Reports*, vol. 44. no. 3. (1979) 691-694.

[539] REBECCA L. LOEFFLER AND TIMOTHY J. LAWSON, 2002, pp. 291-292.

[540] e.g., see. DARRELL STEFFENSMEIER AND STEPHEN DEMUTH, 2006, pp. 256-258; BYUNGBAE KIM, XIA WANG AND HYUNJUNG CHEON, 2018, pp. 489-495; KELSEY L. KRAMER AND XIA WANG, 2019, pp. 1303-1307; DARRELL STEFFENSMEIER, JOHN KRAMER AND JEFFERY ULMER, 1995, p. 600; BARBARA A. KOONS-WITT, ERIC L. SEVIGNY, JOHN D. BURROW AND RHYS HESTER, 2014, pp. 299-324; DARRELL STEFFENSMEIER, NOAH PAINTER-DAVIS AND JEFFERY ULMER, 2017, pp. 821-828; JEFFREY S NOWACKI: An intersectional approach to race/ethnicity, sex, and age disparity in

male or female rather than the differentials of sentencing outcomes. For instance, Richards, Smith, Jennings, Bjerregaard, and Fogel, in their project to examine the 'sex matters' in capital sentencing, demonstrated the probability of the death penalty's imposition is significantly varying between male and female in the involved cases.[541]

The third extralegal factor, which is always with more interactive research, under the United States' contextual environment, is race/ethnics. As aforementioned, China's race/ethnics discrimination problem is not on a relatively problematic level, like in the United States. However, the race/ethnics discriminative problem, to some extent, represents the attitude of the mainstream majority against the minority. The current research or further researches on the sentencing disparity in China's legal practice could also learn a lesson from the research pattern of the race/ethnics minority research in the United States. To summarize the existed findings of correlated researches, the central idea is that minorities, represented by Blacks and Hispanics, are generally disadvantaged in sentencing outcomes compared with mainstream Whites. Although the studies' results are roughly the same, there are some differences in research ideas among different studies. For example, beyond the Black-White classification, Burch launched research based on the skin color to focus on more details in the sentencing disparity;[542] Franklin turned research foci from traditional Whites, Blacks, and Hispanics to the native Americans and paid more attention to the small minority.[543] Furthermore, in comparison with the research that focuses only on the impact of racial/ethical situations, such as Lynch and Haney[544], Free[545], and Bales and Piquero[546], from a purely quantitative point of view, the interactive study of race and other extralegal factors occupies a

federal sentencing outcomes: An examination of policy across time periods. *Criminology & Criminal Justice*, vol. 17. no. 1. (2017) 97-116; KATHLEEN DALY AND REBECCA L. BORDT: Sex Effects and Sentencing: An Analysis of the Statistical Literature. *Justice Quarterly*, no. 1. (1995) 141-176; GRANT A. BROWN: Gender as a factor in the response of the law-enforcement system to violence against partners. *Sexuality and Culture*, vol. 8. no. 3. (2004) 3-139.

[541] TARA N. RICHARDS, M. DWAYNE SMITH, WESLEY G. JENNINGS, BETH BJERREGAARD AND SONDRA J. FOGEL, 2014, pp. 681-697.

[542] TRACI BURCH, 2015, pp. 402-404.

[543] TRAVIS W. FRANKLIN: Sentencing Native Americans in US Federal Courts: An Examination of Disparity. *Justice Quarterly*, vol. 30. no. 2. (2013) 310-339.

[544] MONA LYNCH AND CRAIG HANEY: Discrimination and Instructional Comprehension: Guided Discretion, Racial Bias, and the Death Penalty. *Law and Human Behavior*, vol. 24. no. 3. (2000) 337-358.

[545] MARVIN D. FREE, 2001, pp. 199-219.

[546] WILLIAM D. BALES AND ALEX R. PIQUERO: Racial/Ethnic Differentials in Sentencing to Incarceration. *Justice Quarterly*, vol. 29. no. 5. (2012) 742-773.

considerable proportion in the study of this factor.[547]

The other extralegal factors impacting sentencing outcomes, such as education, socioeconomic status, occupation status, and marital status, have also been discussed in different literature. For example, Franklin, Dittmann, and Henry examined the disparities of defendants' educational background as a contributing factor to the probability of getting an intermediate sanction.[548] They found that the educational background could play a measurable role in the application of intermediate sanctions. As for the socioeconomic status, Benson and Walke[549] "found no significant relationship between the defendant's socioeconomic status and sentence severity."[550] However, whether a specific factor could influence the sentencing or not while putting all factors above together and treating them as a whole, it could infer that the extralegal factors test on the functioning of intrusion of sentencing has been proven by many quantitative or qualitative types of research which are valuable and inspired.

2.2 THEORETICAL FRAMEWORKS ON EXPLAINING SENTENCING DISPARITY

When initiating empirical researches, scholars invariably seek specific theoretical frameworks to explain or legitimate their findings in the study. The research of sentencing disparity is no exception. Researchers in this arena had deployed many theoretical

[547] e.g., see. DARRELL STEFFENSMEIER AND STEPHEN DEMUTH, 2006, pp. 256-258; JEFFERY T. ULMER, JAMES EISENSTEIN AND BRIAN D. JOHNSON, 2009, pp. 569-573; FRANK MCINTYRE AND SHIMA BARADARAN, 2013, pp. 743-747; NOAH PAINTER-DAVIS AND JEFFERY T. ULMER, 2019, pp. 13-15; ED A. MUNOZ AND ADRIENNE B. FRENG, 2008, pp. 38-45; JILL K. DOERNER AND STEPHEN DEMUTH, 2010, pp. 7-11; ERIC P. BAUMER, 2013, pp. 255-256; DARRELL STEFFENSMEIER, JOHN KRAMER AND JEFFERY ULMER, 1995, pp. 588-591; BARBARA A. KOONS-WITT, ERIC L. SEVIGNY, JOHN D. BURROW AND RHYS HESTER, 2014, pp. 299-324; DARRELL STEFFENSMEIER, NOAH PAINTER-DAVIS AND JEFFERY ULMER, 2017, pp. 818-819; JEFFREY S NOWACKI, 2017, pp. 97-116; OJMARRH MITCHELL: A Meta-Analysis of Race and Sentencing Research: Explaining the Inconsistencies. *Journal of Quantitative Criminology*, vol. 21. no. 4. (2005) 439-466; BRETT C. BURKHARDT: Criminal Punishment, Labor Market Outcomes, and Economic Inequality: Devah Pager's Marked: Race, Crime, and Finding Work in an Era of Mass Incarceration. *Law & Social Inquiry*, vol. 34. no. 4. (2009) 1039-1060; MONA LYNCH AND MARISA OMORI: Crack as Proxy: Aggressive Federal Drug Prosecutions and the Production of Black–White Racial Inequality. *Law & Society Review*, vol. 52. no. 3. (2018) 773-809.

[548] TRAVIS W FRANKLIN, LAYNE DITTMANN AND TRI KEAH S HENRY: Extralegal disparity in the application of intermediate sanctions: An analysis of US district courts. *Crime & Delinquency*, vol. 63. no. 7. (2017) 839-874.

[549] MICHAEL L. BENSON AND ESTEBAN WALKER: Sentencing the White-Collar Offender. *American Sociological Review*, vol. 53. no. 2. (1988) 294-302.

[550] CELESTA A. ALBONETTI: Judicial Discretion in Federal Sentencing: An Intersection of Policy priorities and Law. *Criminology & Public Policy*, vol. 10. no. 4. (2011) 1151-1155.

frameworks to understand the sentencing disparity, such as Uncertainty Avoidance Theory, Causal Attribution Theory, Focal Concerns Theory, the Chivalry, the Evil Women Perspectives, Social Worlds Framework, and Organizational Contexts Perspective.

Albonetti tried to incorporate the Uncertainty Avoidance Theory and the Causal Attribution Theory to explain judicial discretion.[551] On the one hand, the Structural Organizational Theorists believe that complete knowledge could eliminate the uncertainty in decision-making.[552] On the other hand, the reality is that the judges are generally unable to get all the offenders' useful information, especially unable to predict future criminal behaviors accurately. The judges in the sentencing process have to rely on some pattern responses, stereotypes, which are usually linked to the offenders' characteristics, such as age, gender, and race, to manage the uncertainty.[553] Casual Attribution theory could play a significant role in sentencing. When applying factors such as the offenders' characteristics, crime scenarios, and pre-trial process results to assess the offenders' future conducts, "attributions of a stable and enduring disposition are expected to increase sentence severity, or of a temporary or situational involvement in crime are expected to decrease sentence severity."[554]

Another prevalent theory to understand the sentencing disparity in the legal practice is the Focal Concerns Theory. This theory has been described as the "hegemonic" theoretical framework to interpret demographic and other sentencing disparities with the bulk of criminological research.[555] Focal concerns first appeared in the social science literature, which researched the gang delinquency with the lower-class culture.[556] The first application of this framework in criminological research was about parole release decision-making.[557] Then, in 1998, this theory was first fully elaborated in the research of sentencing disparity.[558] Two prongs are constructed in this research: one is about the particular concerns in

[551] CELESTA A. ALBONETTI: An Integration of Theories to Explain Judicial Discretion. *Social Problems*, vol. 38. no. 2. (1991) 247-266.

[552] HERBERT A. SIMON: *Administrative behavior: A study of decision-making processes in administrative organizations*. New York, Macmillan, 1957.

[553] CELESTA A. ALBONETTI, 1991, pp. 248-250.

[554] CELESTA A. ALBONETTI, 1991, pp. 248-250.

[555] MONA LYNCH: Focally Concerned About Focal Concerns: A Conceptual and Methodological Critique of Sentencing Disparities Research. *Justice Quarterly*, vol. 36. no. 7. (2019) 1148-1175.

[556] WALTER B. MILLER: Lower class culture as a generating milieu of gang delinquency. *Journal of Social Issues*, vol. 14. no. 3. (1958) 5-19.

[557] MONA LYNCH, 2019, pp. 1149-1153; PETER B. HOFFMAN: Paroling policy feedback. *Journal of Research in Crime and Delinquency*, vol. 9. no. 2. (1972) 117-131.

[558] DARRELL STEFFENSMEIER, JEFFERY ULMER AND JOHN KRAMER, 1998, pp. 766-769.

sentencing decision-making; the other is about the cognition and context which could generate the disparities. Under these two prongs of the focal concern theory, three concerns were built, i.e., blameworthiness, protection of community safety, and Practicality / Organizational Implications.

Blameworthiness roots in the defendants' culpability and looks forward to making the punishment fitting the crime. Protection of community safety emphasizes the incapacitation and general deterrence, and meanwhile, considers the offenders' future behaviors, like recidivism. Practicality / Organizational Implications pay much attention to the constraints of the offenders or organizational problems.[559] The significance of extracting these three focus concerns from sentencing practice is that, on the one hand, they imply a dichotomy of the influencing factors of legally-relevant and extralegal factors. On the other hand, these three focus concerns implicitly involve individual subjective evaluations. Though some evaluations could arguably be constrained by sentencing guidelines, with combining the theories of uncertainty avoidance and casual attribution above, there is still much room left for stereotypes and heuristic cognitive models.

For this reason, many pieces of research applied this model to conceptualize and operationalize the variables.[560] However, there are still some challenges to the focal concerns theory's aptness to explain the sentencing complexity. From the operationalized viewpoint, the legally-relevant factors, such as criminal history, are generated by inequality; the value of distinction is undermined.[561] Furthermore, the initial focal concerns theory aims at explaining the group-level phenomena. However, the recent research deploys and develops this theory to an individualistic approach, which pays more attention to its characteristics. Murakawa and

[559] DARRELL STEFFENSMEIER AND NOAH PAINTER-DAVIS: Focal Concerns Theory as Conceptual Tool for Studying Intersectionality in Sentencing Disparities: Focus on Gender and Race along with Age. In: JEFFERY T. ULMER AND MINDY S. BRADLEY (eds): *Handbook on Punishment Decisions: Locations of Disparity*. New York, Routledge, 2017. 189-210.

[560] e.g., see. DARRELL STEFFENSMEIER AND STEPHEN DEMUTH, 2006, pp. 245-247; KELSEY L. KRAMER AND XIA WANG, 2019, pp. 1286-1290; NOAH PAINTER-DAVIS AND JEFFERY T. ULMER, 2019, pp. 13-15; JILL K. DOERNER AND STEPHEN DEMUTH, 2010, pp. 8-11; DARRELL STEFFENSMEIER, NOAH PAINTER-DAVIS AND JEFFERY ULMER, 2017, pp. 818-819; JEFFREY S NOWACKI, 2017, pp. 97-116; GEOFF WARD, AMY FARRELL AND DANIELLE ROUSSEAU: Does Racial Balance in Workforce Representation Yield Equal Justice? Race Relations of Sentencing in Federal Court Organizations*. *Law & Society Review*, vol. 43. no. 4. (2009) 757-806.; XIA WANG, DANIEL P. MEARS, CASSIA SPOHN AND LISA DARIO: Assessing the Differential Effects of Race and Ethnicity on Sentence Outcomes Under Different Sentencing Systems. *Crime*, vol. 59. no. 1. (2013) 87-114.

[561] MONA LYNCH, 2019, p. 1157.

Beckett[562] criticized that "[T]he individualistic approach to the social scientific study of racial inequality in the criminal justice study rests on an incorrect assumption that the system itself is racially innocent and that only individual bad acts produce the problem of biased outcomes."[563] As for explaining the function of race biases to sentencing outcomes, Lynch asserted that implicit bias would be better to have an impact than explicit biases, which measured under the Steffensmeier's focal concerns theory translation, on the sentencing outcomes. The theory of "aversive racism"[564] could be applied to better understand the racial impacts, as promoted by Lynch. The critique seems to sway the foundation of the three focal concerns. Nonetheless, the focal concerns theory still could have a good fitting with some adjustments in explaining the demographic characteristics' disparities.

The Chivalry and the Evil Women Perspectives were usually taken for explaining the gender-based disparities.[565] The chivalry emphasized the paternalistic demand in male court actors to protect the female. Under this perspective, female offenders have a high likelihood of getting lenient outcomes compared with male ones.[566] Kramer and Wang[567] elucidate that, as for the perspective of Evil Women, "female offenders who fail to meet traditional gender expectations or/and commit more masculine, violent crimes are treated either no different or more harshly than males who commit the same crimes."[568]

The Social Worlds Framework and Organizational Context Perspective do a relatively

---

[562] NAOMI MURAKAWA AND KATHERINE BECKETT: The Penology of Racial Innocence: The Erasure of Racism in the Study and Practice of Punishment. *Law & Society Review*, vol. 44. no. 3-4. (2010) 695-730.

[563] MONA LYNCH, 2019, p. 1157.

[564] JOHN F. DOVIDIO AND SAMUEL L. GAERTNER: The aversive form of racism. In: JOHN F. DOVIDIO AND SAMUEL L. GAERTNER (eds): Prejudice, discrimination, and racism. Orlando, FL, Academic Press, 1986.

[565] e.g., see. ILENE H. NAGEL AND JOHN HAGAN: Gender and crime: Offense patterns and criminal court sanctions. *Crime and Justice*, vol. 4. (1983) 91-144; TIMOTHY GRIFFIN AND JOHN WOOLDREDGE: Sex-Based Disparities in Felony Dispositions Before Versus After Sentencing Reform in Ohio. *Criminology*, vol. 44. no. 4. (2006) 893-923; NATALIE GOULETTE, JOHN WOOLDREDGE, JAMES FRANK AND LAWRENCE TRAVIS: From Initial Appearance to Sentencing: Do Female Defendants Experience Disparate Treatment? *Journal of Criminal Justice*, vol. 43. no. 5. (2015) 406-417.

[566] TIMOTHY GRIFFIN AND JOHN WOOLDREDGE, 2006, pp. 893-923; NATALIE GOULETTE, JOHN WOOLDREDGE, JAMES FRANK AND LAWRENCE TRAVIS, 2015, pp. 406-417; MARGARET FARNWORTH AND JR RAYMOND H. C. TESKE: Gender Differences in Felony Court Processing. *Women & Criminal Justice*, vol. 6. no. 2. (1995) 23-44.

[567] KELSEY L. KRAMER AND XIA WANG, 2019, p. 1287.

[568] e.g., see. BARBARA A. KOONS-WITT, ERIC L. SEVIGNY, JOHN D. BURROW AND RHYS HESTER, 2014, pp. 299-324; ILENE H. NAGEL AND JOHN HAGAN, 1983, pp. 91-144; CORTNEY A. FRANKLIN AND NOELLE E. FEARN: Gender, race, and formal court decision-making outcomes: Chivalry/paternalism, conflict theory or gender conflict? *Journal of Criminal Justice*, vol. 36. no. 3. (2008) 279-290.

rare appearance in the research of sentencing disparities. Social Worlds Framework contends that every social world has at least one primary activity, unique sites, and a technology that is either inherited or innovative to carry out its activities.[569] The group members of one social world will share the resources of many kinds to achieve their goals. If one treats the criminal court as one social world, this social world's goal would be to reach sentencing outcomes. The judges would share the sentencing guidelines as technology. However, both the meaning and utilization of a sentencing guideline would alter saliently between different criminal courts within any given jurisdiction.[570] It could be sentencing disparity caused by the factor of the locale, which is an extralegal factor. The organizational context perspective concludes in a similar way that individual sentencing outcomes adjudicated by any criminal court are influenced by the political, social, and organizational context of that court.[571]

The current research expects to find the results to support the reviewed theories above. According to the research questions, this study will pay more attention to the Focal Concerns Theory, the Chivalry perspective, and Uncertainty Avoidance Theory, but with cautions on the other theories.

3. METHODOLOGY

3.1 DATA AND SAMPLING

The current study's objective is to find whether the sentencing disparities exist in the sentencing outcomes of the auxiliary cybercrime in China. According to this objective, this study's data was drawn from the real cases that appeared in the form of judgment on the China Judgements Online (CJO) website. In 2016, the Supreme People's Court of China enacted a judicial interpretation that stipulated that courts on every hierarchy level should publicize and upload all the adjudicated judgments to the CJO[572], which provides an opportunity to research real cases. On the one hand, judgments generally contain much information, such as the offender's name, gender, residence, nationality, educational level, occupational status, and ID number. Despite this, the Supreme People's Court stipulated that personal information, ID number, and some law information should be deleted when

[569] ADELE CLARKE AND SUSAN STAR: The Social Worlds Framework: A Theory/Methods Package. In: EDWARD J HACKETT, OLGA AMSTERDAMSKA, MICHAEL LYNCH AND JUDY WAJCMAN (eds): *The Handbook of Science and Technology Studies*. Cambridge, M.I.T. Press, 2008. 113-137.

[570] PAULA M. KAUTT, 2008, pp. 267-270.

[571] PAULA M. KAUTT, 2008, pp. 267-270.

[572] SUPREME PEOPLE'S COURT: *Provisions on People's Courts Publishing Judgment Documents on the Internet*, 31 August 2016, http://www.court.gov.cn/zixun-xiangqing-25321.html

publishing and uploading judgments to the CJO. Nevertheless, there is still much information about the characteristics of the offenses and information related to offenders classified into offenders' characteristics.

On the other hand, because auxiliary cybercrimes are codified by criminal law since September 2015, the current study's data collection covers September 2015 to September 2019. The current study could collect 168 pieces of judgment covering 273 defendants and sentencing outcomes by filtering those uploaded judgments. The defendants' information is not integrated, and those without sentencing outcomes (this could be a technical problem that part of the judgment with unexpected uploading failure). As aforementioned, the official statistics showed that, in the same period, there were 260 cases and 473 defendants involved. The current study extracted nearly 57.7% effective sentencing outcomes.

Though the sampling occupied a large proportion of the sentencing outcomes, the sample size is still small, limiting by research object, auxiliary cybercrime, compared with other researches of sentencing disparity. In mathematical operation, the small sample will decrease the statistical power, making some crucial variables lack significance in the results and further mislead the conclusions.[573] However, confined by reality, the current study has to bear these limitations and tries to overcome them by variables' setting.

3.2 VARIABLES

In the current research, variables are classified into factors and sentencing outcomes from a macro-level. This study divided factors into two sub-categories: legally-relevant factors stipulated in the Criminal Law Code and Sentencing Guidelines as legal sentencing scenarios and extralegal factors that are not legitimated in those two documents.

The current study's dependent variable is the offenders' sentencing outcome, consisting of incarceration length, amounts of fines, and probation application. According to the Criminal Law Code of China, there are two types of criminal punishments: principal punishments and supplementary punishments.[574] The types of principal punishments are (1) public surveillance, (2) criminal detention, (3) fixed-term imprisonment, (4) life imprisonment, and (5) the death penalty.[575] The types of supplementary punishments are (1)

[573] CHRIS DEZIEL: *The Effects of a Small Sample Size Limitation*, 13 March 2018, https://sciencing.com/effects-small-sample-size-limitation-8545371.html

[574] see. Article 32 of the *Criminal Law*.

[575] see. Article 33 of the *Criminal Law*.

fines, (2) deprivation of political rights, and (3) confiscation of property.[576] As for the current research object, the auxiliary cybercrime, which consists of two articles in China's Criminal Law, both articles have the same sentencing range or statutory sentencing results. As written in the Criminal Law, whoever commits an auxiliary cybercrime should be sentenced to imprisonment of not more than three years, or criminal detention, in addition to a fine, or should be sentenced to a fine only.

Given that the imprisonment and the criminal detention are both considered incarcerations applied to offenders – with different units of measurement as the former is measured by the year and the latter by the month – the current research unified these two types of sentences into a new dependent variable, Incarceration Length, measured by the unit of the month, for the convenience of measurement. The minimum one represents the offenders sentenced only to *Fines*. The maximum one is "36," according to the law. Then, the incarceration length ranges from 0 to 36-month. After data collection, the current study found that every sentencing resulted in a fine. Another dependent variable, the Amounts of Fines, directly extracts from the judgments and sets as a scale variable. As for probation, some scholars treat it as an independent sentencing outcome.[577] The current study followed this idea and set the Application of Probation as a dependent variable, coded as a dummy variable with "0" (Not applied) and "1" (Applied).

The independent variables in the current research are those factors that could have an impact on the sentencing outcomes. As discussed above, all these factors are divided into legally relevant factors and extralegal factors. In this study, the legally relevant factors include two types of variables: Case Facts and Crime Seriousness; the extralegal factors also include Systematic Features and Offenders' Characteristics.

Case Facts mainly depend on the criminal conduct of the auxiliary cybercrime. The current study focuses on the criminal conduct stipulated in the Criminal Law Code for the statutory sentencing range, and results are the same in both types of auxiliary cybercrime. The variable of criminal conduct is coded as a nominal variable. The value in this variable respectively represents the different criminal conducts: setting website or communication group for crimes (coded as 1), sending illegal information in the cyberspace (coded as 2), sending messages for fraud and other crimes (coded as 3),[578] providing technical support for

[576] see. Article 34 of the *Criminal Law*.
[577] e.g., see. NORVAL MORRIS AND MICHAEL TONRY, 1991; XINGHONG ZHAO, 2016, pp. 46-61.
[578] see. Article 287(I) of the *Criminal Law*.

crimes in the cyberspace (coded as 4), and assisting the cyber-criminals by offering advertisement, payment method, or other assistance (coded as 5).[579]

Crime Seriousness in the current study contains unit crime, joint crime, identity in the crime, and convergence of other crimes. The unit crime could be simply understood as corporate crime. Generally, the unit crime involves multi-offenders, so according to the sentencing guideline, the punishment for the unit crime perpetrators would arguably be harsher than single offenders'. In this study, the unit crime is coded as a dummy variable with "0" (No) and "1" (Yes). The joint crime in the Criminal Law of China refers to the circumstance that two (or more) offenders intentionally commit a crime. As the unit crime, the joint crime would arguably be sentenced harsher. The joint crime is coded as a dummy variable with "0" (No) and "1" (Yes). The crime's identity is based on the concept of complicity, which consists of principals and accomplices. Accomplices could get more lenient sentencing outcomes than principals.[580] For those cases that could not be considered a joint crime, this study applied the following strategy: if a case only involved one offender, then that offender was considered the principal of the crime. The joint crime is coded as a dummy variable as the previous two. The last variable of Crime Seriousness is the convergence of other crimes. As discussed before, the auxiliary cybercrime has an independent criminal law status as it is separated from a previously committed crime. In other words, whether the supportive conduct promotes another crime or not, the supportive conduct itself is convictable. In turn, if the offender of the auxiliary cybercrime facilitates the commission of other crimes, the crime is more severe than in the case of those crimes that do not. The convergence of other crimes is coded as a dummy variable, as well. These four variables are also aggravating circumstances in the sentencing; the current study summed the value of them as a comprehensive ordinal variable to evaluate the aggregating crime seriousness, named Crime Seriousness. As for the mitigating circumstances, because all the offenders involved in this study accepted guilty and performed remorse, the function thereof was not considered. The Crime Serious range is from 1(only one offender committed the crime without the convergence of other crimes) to 4 (the maximum involved all four previous variables).

Systematic Features in this research predominantly consider the location of the court. In general, the court in a specific locale has jurisdiction over the crimes in this area. During

[579] see. Article 287(II) of the *Criminal Law*.

[580] see. Article 27 of the *Criminal Law*.

the same examined period, if one kind of crime was judged more often in place A than in place B, then it could be the case that the crime density is more significant in place A than in place B. So, the location of the court is an indicator of the crime rate to some extent. As mentioned before, one of the research questions is about the regional disparities in the sentencing outcomes of auxiliary cybercrime. The current research collected the court location's regional information and coded them as the nominal variable in China's provinces. After data collection and variables codification, the current research found that the auxiliary cybercrime's provincial distribution is significantly discrete. Second, the research question's underlying expectation is to find whether the regional disparities or discrimination would influence the sentencing outcomes. Third, because of the regional disparities or discrimination might be the connotation of the economic disparities. Then, for better revealing the regional disparities and moderating the discrete distribution, the current study classified the 31 provinces in the China mainland into five regions based on the provincial per capita GDP in the fiscal year of 2018. According to the statistical numbers given by the National Bureau of Statistics of China[581], the current study coded the rank 1-7 of per capita GDP province as "5" (Regions: high per capita GDP), the rank 8-13 as "4" (Regions: fairly high per capita GDP), the rank 14-19 as "3" (Regions: high per capita GDP), the rank 20-25 as "2" (Regions: fairly low per capita GDP), and the rank 26-31 as "1" (Regions: low per capita GDP).

Offenders' Characteristics in this research consist of the following factors: gender, age, residence, and educational level. Gender in this study is coded as a dummy variable with "0" (female) and "1" (Male). The age in this study represents the offenders' age when they were sentenced. It is calculated by the date of the trial and the birthday of the offenders. In the preliminary disposition, the minimum value is 18, while the maximal value is 56. Considering the findings in the research of Steffensmeier, Kramer, and Ulmer[36] that Age has a curvilinear relationship to sentencing with offenders in their 20s and early 30s sentenced most harshly, while offenders in their 50s or older received extraordinarily lenient sentences. Falling between these two extremes were teen-adults (18-20) and offenders in their late 30s and 40s." The current study categorized age into four ranks. Age within 18-24 is coded as 1, 25-29 is coded as 2, 30-35 is coded as 3, and age at/above 36 is coded as 4. The variable of residence has the same codification as the Court Location above. As for the level of education,

[581] NATIONAL BUREAU OF STATISTICS OF CHINA: Gross Regional Product (2018) [地区生产总值（2018）]. In: SHENGYONG MAO AND ZHICAI YE (eds): *China Statistical Yearbook-2019* [中国统计年鉴 2019]. Beijing, China Statistics Press, 2019.

though much research has proven its impact on the sentencing outcome, it still needs to test in China's content.

Furthermore, as this study's object is the auxiliary cybercrime, which has been treated as a high-technology crime[582], it is reasonable to link the level of education to the capacity to commit a cybercrime. On the other hand, there is a traditional cultural perspective with significant influence in Chinese society: "for those who know the law and violate the law, they should be punished harsher." People with high educational levels are inferred to know the law better than those with low educational levels and should be punished harsher when committing a crime. With these considerations, the Educational Level is coded as an ordinal variable with "1" (Primary School), "2" (Middle School), "3" (High School), and "4" (College and above).

3.3 Analytical Strategy

The current research has been launched in two steps. First, to check the effects on the sentencing outcomes, this study put all the independent variables into the analysis with the Multivariate Analysis method. The dependent variables are sentencing outcomes of probation, incarceration length, and the amounts of fines. Second, this study applied the Binary Logistic Regression and Hierarchical Linear Regression Analysis methods to test the variables' far-reaching influence on sentencing outcomes. The strategy here is to add the extralegal factors into the regression model and check the significance, then put the legally relevant factors into the model and check how much of variance has been explained and which extralegal factor is still with statistical significance. Then, the disparities within these factors might be the causes of the sentencing disparities.

4. Findings

4.1 Descriptive Analyses

Table V. 4.1-1 provides descriptive statistics for all the variables contained in the current study. According to the trial's variable statistics, the sentencing outcomes of offenders distributed discretely within this sample. More than half (50.5%) of the sentencing outcomes were given in 2018. The count of sentencing outcomes has a significant increasing trend by year in this sample. However, this study's data only counted to September 2019, so the number of sentencing outcomes in 2019 did not maintain this trend. The criminal

[582] e.g., GERALD L KOVACICH AND WILLIAM C BONI: *High-technology crime investigator's handbook: establishing and managing a high-technology crime prevention program*. Elsevier, 2011.

conducts of the auxiliary cybercrime are of homogenous distribution in this sample. In this

Descriptive Statistics of Variables

Variables		Count	Valid N %	Median	Mean	SD
Trial Year	2015	2	0.7%			
	2016	11	4.0%			
	2017	44	16.1%			
	2018	138	50.5%			
	2019	78	28.6%			
Crime Conduct	1	54	19.8%			
	2	50	18.3%			
	3	20	7.3%			
	4	53	19.4%			
	5	96	35.2%			
Unit Crime	No	218	79.9%			
	Yes	55	20.1%			
Joint Crime	No	148	54.2%			
	Yes	125	45.8%			
Identity in Crime	Compliance	59	21.6%			
	Principal	214	78.4%			
Convergence	No	184	67.4%			
	Yes	89	32.6%			
Crime Seriousness	1	114	41.8%			
	2	108	39.6%			
	3	51	18.7%			
Court Location	1	18	6.6%			
	2	22	8.1%			
	3	65	23.8%			
	4	26	9.5%			
	5	142	52.0%			
Gender	Female	44	16.1%*			
	Male	229	83.9%			
Age	18-24	57	20.9%			
	25-29	106	38.8%			
	30-35	83	30.4%			
	36-	27	9.9%			
Age of Perpetrators				28.00	28.85	5.60
Educational Level	Primary	16	5.9%			
	Middle	95	34.8%			
	High	66	24.2%			
	College	96	35.2%			
Offender's Region	1	34	12.5%			
	2	41	15.0%			
	3	50	18.3%			
	4	29	10.6%			
	5	119	43.6%			
Probation Application	Not Applied	199	72.9%			
	Applied	74	27.1%			
Incarceration Length				10.00	11.25	6.22
Amounts of Fine				10000.00	23611.36	42318.03

Table V. 4.1-1 Descriptive Statistics of Variables

sample, 20.1% of cases are a unit crime, while 79.9% are not. 45.8% of cases are a joint crime. Compared with the findings in the official report on general cybercrime, the rate of a joint crime is 43.22%[583], the rate of a joint crime in this sample is consistent with that finding by T-test (t=.850, p=.396, α=.05). The crime seriousness score calculated by the unit crime variables, the joint crime, the identity in crime, and convergence, ranged from 1 to 3; and 80.4% of cases were at the interval of 1-2.

As for the extralegal factor of the court's location showed that over half (52.0%) of the cases were sentenced in region 5 (a region with high per capita GDP)[584], and 18.7% of the cases were sentenced in region 3 (a region with average per capita GDP)[585]. Gender distribution in this study is that 83.9% of the offenders are male, while 16.1% are female. However, combined with the integral female criminal rate of 9.3% of all kinds of crimes [586], the current study found that the female criminal rate of auxiliary cybercrime is not consistent with, or higher than, the integral female criminal rate through T-test (t=3.058, p=.002, α=.05). In the current study, Age∈[18,56] (Mean=28.85, σ=5.6, Mode=29) has no significant difference with 28, offered by the official statistics of all the general cybercrime.[587] In terms of education level and offender's region, the offenders in this study were mainly those with a middle school diploma (34.8%) and a college degree or above (35.2%); and most (43.6%) of them come from the high per capita GDP region.

As for the variables of sentencing outcomes in this study, 27.1% of offenders involved got probation. The probation rate in the auxiliary cybercrime sentencing is consistent with the integral probation application rate (27.4%) offered by China's legal yearbook through the T-test (t=-.109, p=.913, α=.05). In terms of the incarceration length and the amounts of fines, the incarceration length∈ [0,30] (Mean=11.25, σ=6.22); and the amount of fines∈ [1,000, 400,000] (Mean= 23611.35, σ=42318.03).

To sum, from several critical indicators, this study's sample can arguably well reflect the trend of cybercrime and the current situation of penalty application in China.

---

[583] CHINA JUSTICE BIG DATA ACADEMY, 2019.

[584] Region 5 (a region with high per capita GDP) includes 7 regions in China: Beijing, Shanghai, Tianjin, Jiangsu, Zhejiang, Fujian, and Guangdon

[585] Region 3 (a region with average capita GDP) includes 6 regions in China: Jilin, Ningxia, Hunan, Hainan, Henan, and Xinjiang.

[586] XIAOMEI WU: *Law Yearbook of China-2018*. Beijing, Press of Law Yearbook of China, 2018.

[587] CHINA JUSTICE BIG DATA ACADEMY, 2019.

4.2 RESULTS OF MULTIVARIATE TESTS

Multivariate Tests of Between-Subjects Effects

Factors	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	*p.*
Corrected Model	Probation Application	7.607[a]	21	.362	1.962	.008*
	Imprisonment Length	2793.350[b]	21	133.017	4.316	.000*
	Amount of Fine	60829844208.717[c]	21	2896659248.034	1.706	.030*
Intercept	Probation Application	3.122	1	3.122	16.912	.000*
	Imprisonment Length	5523.914	1	5523.914	179.222	.000*
	Amount of Fine	18541926289.039	1	18541926289.039	10.918	.001*
Conduct	Probation Application	1.220	4	.305	1.653	.162
	Imprisonment Length	153.425	4	38.356	1.244	.293
	Amount of Fine	1719635365.323	4	429908841.331	.253	.908
Seriousness	Probation Application	.241	2	.121	.653	.521
	Imprisonment Length	551.337	2	275.668	8.944	.000*
	Amount of Fine	6512025705.109	2	3256012852.555	1.917	.149
Court Location	Probation Application	2.050	4	.513	2.777	.028*
	Imprisonment Length	585.733	4	146.433	4.751	.001*
	Amount of Fine	14846179200.095	4	3711544800.024	2.185	.071
Gender	Probation Application	.000	1	.000	.001	.981
	Imprisonment Length	286.976	1	286.976	9.311	.003*
	Amount of Fine	59747547.998	1	59747547.998	.035	.851
Age1	Probation Application	.540	3	.180	.975	.405
	Imprisonment Length	137.109	3	45.703	1.483	.220
	Amount of Fine	9184013726.548	3	3061337908.849	1.803	.147
Education	Probation Application	.247	3	.082	.446	.721
	Imprisonment Length	84.010	3	28.003	.909	.437
	Amount of Fine	3904036725.012	3	1301345575.004	.766	.514
Region	Probation Application	1.852	4	.463	2.509	.043*
	Imprisonment Length	381.760	4	95.440	3.097	.016*
	Amount of Fine	6836184819.601	4	1709046204.900	1.006	.405

a. R^2= .141; b. R^2= .265; c. R^2 = .125; *. p<0.05

Table V. 4.2-1 Multivariate Tests of Between-Subjects Effects

According to the analytic strategy, the current study first put all the independent variables into the multivariate tests model for checking the subject effects of them on the sentencing outcomes, the probation application, the incarceration length, and the amounts of fines.

As reported in Table V. 4.2-1, the current study got some findings: first, as for the subject effect of independent variables on the probation application, the general linear model of the probation application has statistical meaning (R^2=.141, F=1.962, p=.008, α=.05). As the legally relevant variables, the criminal conduct and the crime seriousness had no

statistically significant influence on the probation application. Regarding the extralegal factors, gender, age, and educational level had no statistically significant effects on the sentencing's probation application. However, the court location (F=2.777, p=.028, α=.05) and the offender's region (F=2.509, p=.043, α=.05), the other two extralegal factors, were with significant effects on the probation application. Second, in the general linear model of incarceration length, which as well had the statistical meaning (R^2=.265, F=4.316, p=.000, α=.05), the crime seriousness (F=8.944, p=.000, α=.05) had very significant effects on the incarceration length, whereas the criminal conduct had no significant ones. The age and educational level of extralegal factors still had no significant effects on the incarceration length. However, the other extralegal factors, the gender (F=9.311, p=.003, α=.05), the court location (F=4.751, p=.001, α=.05), and the offender's region (F=3.097, p=.016, α=.05) revealed a significant correlation with the incarceration length. The last, in the general linear model of amounts of fines, though also was with the statistical significance (R^2=.125, F=1.706, p=.030, α=.05), all the independent variables from either legally relevant factors or extralegal factors had no statistically significant correlations with the amounts of fines.

In the first stage of the multivariate tests, the current study found some independent variables that could arguably affect the sentencing outcomes. This study then expects to test the coefficients between sentencing outcomes and differentials within a particular independent variable, under the presumption that all the variables might affect the sentencing outcomes, some findings in Table V. 4.2-2.

First, in terms of the probation application and the differentials within the variable value, as reported in Table V. 4.2-2, the current study had two findings. The offender who committed criminal conduct 1[588] has less likelihood to be put on probation (B=-.207, t=-2.518, p=.012, α=.05) than those who committed criminal conduct 5. The other one is that the offender sentenced in a low per capita GDP region court (B=-.258, t=-2.125, p=.035, α=.05) or a fairly high per capita GDP region (B=-.233, t=-2.381, p=.018, α=.05) had less chance to be put on probation than those who sentenced in a high per capita GDP region. Combined with the results in Table V. 4.2-1, the criminal conduct had no statistically significant effects on the probation application. However, according to the current study's hypothesis, the result of the limitation resulting from a small-sized sample of this study made the differentials between criminal conduct 1 and 5 not insignificant in the overall evaluation of the effects of criminal conduct on the probation applications. However, the disparities of probation

[588] Coduct 1: Setting website or communication group for crimes.

application by the court location were further proved in the estimation of the parameters.

Multivariate Test of Parameters Estimation within Variables

	Probation Application			Incarceration Length			Amounts of Fines		
Factors	B	*t*	*p*	B	*t*	*p*	B	*t*	*p*
Intercept	.629	5.609	.000*	15.908	10.985	.000*	37984.377	3.534	.000*
[Conduct=1]	-.207	-2.518	.012*	1.124	1.057	.292	-2356.605	-.299	.766
[Conduct=2]	-.112	-1.311	.191	-.525	-.475	.635	-6195.369	-.757	.450
[Conduct=3]	-.065	-.559	.577	2.362	1.571	.117	-2344.185	-.210	.834
[Conduct=4]	-.100	-1.268	.206	1.009	.988	.324	-6300.599	-.831	.407
[Conduct=5]	0[a]	.	.	0[a]	.	.	0[a]	.	.
[Seriousness=1]	-.075	-.932	.352	-4.350	-4.180	.000*	-13688.308	-1.772	.078
[Seriousness=2]	-.087	-1.105	.270	-2.209	-2.177	.030*	-3712.647	-.493	.622
[Seriousness=3]	0[a]	.	.	0[a]	.	.	0[a]	.	.
[Court Location=1]	-.258	-2.125	.035*	-6.045	-3.847	.000*	-16167.694	-1.386	.167
[Court Location=2]	.066	.636	.526	.938	.698	.486	615.430	.062	.951
[Court Location=3]	-.109	-1.533	.126	-1.661	-1.811	.071	14779.715	2.171	.031*
[Court Location=4]	-.233	-2.381	.018*	-2.017	-1.593	.112	12212.080	1.300	.195
[Court Location=5]	0[a]	.	.	0[a]	.	.	0[a]	.	.
[Gender=0]	-.002	-.023	.981	-3.048	-3.051	.003*	1390.968	.188	.851
[Gender=1]	0[a]	.	.	0[a]	.	.	0[a]	.	.
[Age1=1]	-.181	-1.699	.090	-1.109	-.807	.421	-8490.689	-.832	.406
[Age1=2]	-.119	-1.249	.213	-.175	-.142	.888	2225.208	.243	.808
[Age1=3]	-.103	-1.051	.294	1.053	.828	.409	9497.819	1.006	.315
[Age1=4]	0[a]	.	.	0[a]	.	.	0[a]	.	.
[Education=1]	-.083	-.691	.490	-.740	-.476	.634	-15956.207	-1.383	.168
[Education=2]	-.069	-.939	.349	-.321	-.338	.735	-5619.491	-.799	.425
[Education=3]	-.073	-.979	.328	-1.497	-1.562	.120	-6909.322	-.971	.333
[Education=4]	0[a]	.	.	0[a]	.	.	0[a]	.	.
[Region=1]	-.177	-1.901	.059	1.781	1.476	.141	-5008.939	-.559	.577
[Region=2]	.141	1.646	.101	-2.701	-2.438	.015*	-7748.458	-.942	.347
[Region=3]	.028	.352	.725	-1.167	-1.133	.258	-14503.991	-1.896	.059
[Region=4]	.110	1.164	.246	-1.546	-1.268	.206	-9942.956	-1.099	.273
[Region=5]	0[a]	.	.	0[a]	.	.	0[a]	.	.

a. This parameter is set to zero because it is redundant; *. $p<0.05$

Table V. 4.2-2 Multivariate Test of Parameters Estimation within Variables

Second, regarding the incarceration length and the differentials within the variable value, the current study discovered that (1) in contrast with crime seriousness score 3, offenders whose crime seriousness at 1 (B=-4.350, *t*=-4.180, *p*=.000, α=.05) or 2 (B=-2.209, *t*=-2.177, *p*=.030, α=.05) were more likely to be sentenced less incarceration length, on average, 4.35 months less with former and 2.209 months less with latter; (2) in contrast with the court of location 5, offenders who were sentenced in the court of location 1 (B=-6.045, *t*=-3.847, *p*=.000, α=.05) were sentenced averagely 6.045 months less incarceration length; (3) in contrast with male offenders, female offenders (B=-3.048, *t*=-3.051, *p*=.003, α=.05) were

sentenced averagely 3.048 months less incarceration length; and (5) in contrast with offenders from region 5, those who from the fairly low per capita GDP region-2 (B=-2.701, t=-2.438, p=.015, α=.05)- were sentenced averagely 2.701 months less incarceration length. The findings here comply with the results in Table V. 4.2-1. At this point, it could be preliminarily identified that these four factors will cause sentencing disparities.

Third, concerning the amounts of fines and the differentials within the variable value, the current study observed that, by contrast, offenders who were sentenced in a court of average per capita GDP region (B=14779.715, t=2.171, p=.031, α=.05) could be fined averagely 14,770 yuan more than those in a court of location 5. Regarding the results in Table V. 4.2-1, no variables in this study could affect the amounts of fines. However, here, the court location, to some extent, could influence the fines outcomes. The probable reason to explain this might be the same as the reason discussed above; the limitation is from the sample's small size.

4.3 Results of Regression Analysis

During the first step of the multivariate analyses, the current study preliminarily tested and checked the effects of this study's variables on the sentencing outcomes. For further ascertaining the findings in the multivariate analyses and responding to the research questions or objectives, the second round of tests was conducted on the variables by applying the models of binary logistic regression and hierarchical linear regression. The ordinal logistic regression was applied for exploring the correlation among ordinal and nominal variables. Because the probation application was coded as a binary variable with "Yes" (1) and "No" (0), the binary logistic regression could be a suitable choice. Meanwhile, as sentencing length and amounts of fines are continuous variables, this study applied the hierarchical linear regression. However, whether the binary logistic regression or the hierarchical linear regression is applied here, the strategy is similar, letting the offender's characteristics enter the model. The court location, the last ones are legally relevant factors, the criminal conduct, and crime seriousness, thereby understanding the effects of both extralegal and legally relevant factors on the sentencing outcomes.

Table V. 4.3-1 provides the results of binary logistic regression, which dependent variable is probation application. First, in model 1, let the offender's characteristics, including gender, age, educational level, and offender's region, enter the model. The results of the model's omnibus tests (χ^2=8.168, p=.086, α=.05) expressed that there was no at least one

Binary Logistic Regression of Probation Application

		Omnibus Tests of Model Coefficients			Variables in the Equation			
		Chi-Square	df	*p.*	Variables	B	Exp(B)	*p.*
model 1[a]	Step	8.168	4	.086	Gender	.424	1.529	.295
	Block	8.168	4	.086	Age	.277	1.320	.072
	Model	8.168	4	.086	Education Level	.178	1.195	.243
					Offender's Region	.082	1.086	.416
					Constant	-2.827	.059	.000*
model 2[b]	Step	4.280	1	.039*	Gender	.283	1.328	.496
	Block	4.280	1	.039*	Age	.286	1.332	.068
	Model	12.448	5	.029*	Education Level	.190	1.209	.213
					Offender's Region	.071	1.073	.486
					Court Location	.240	1.271	.046*
					Constant	-3.685	.025	.000*
model 3[c]	Step	4.277	2	.118	Gender	.269	1.309	.522
	Block	4.277	2	.118	Age	.322	1.379	.043*
	Model	16.725	7	.019*	Education Level	.102	1.107	.520
					Offender's Region	.026	1.026	.801
					Court Location	.247	1.280	.040*
					Crime Conduct	.160	1.174	.099
					Crime Seriousness	.203	1.226	.297
					Constant	-4.277	.014	.000*

a. Variable(s) entered in model 1: Gender, Age, Educational Level, Offender's Region.
b. Variable(s) entered in model 2: Court Location.
c. Variable(s) entered in model 3: Crime Conduct, Crime Seriousness.
*. $p.<0.05$

Table V. 4.3 1 Binary Logistic Regression of Probation Application

variable in model 1 that could explain the dependent variable. Then, this study added the court location into the model, i.e., model 2, and found that, on the one hand, model 2 had statistical meaning (χ^2=12.448, p=.029, α=.05); on the other hand, only the court location had the statistically significant effects on the probation application (Exp(B)=1.271, p=.046). Finally, this study added another two legally relevant factors, the criminal conduct and the crime seriousness, into the model, i.e., model 3, and found that: (1) model 3 had the statistical meaning (χ^2=16.725, p=.019, α=.05); and (2) there were two variables, the Age (Exp(B)=1.379, p=.043) and the court location (Exp(B)=1.280, p=.040), in the model 3 could predict the probation application. The value Exp(B) of both Age and court location is more than 1. It means that by the offender's age growing and court location increasing from low per capita GDP region to high per capita GDP region, the offenders were not likely to get the probation. In other words, the younger offenders were with a higher likelihood of getting probation than the old ones; and the offenders who were sentenced in a court of the low per capita GDP region were with more probability of probation application than those in a court

of the high per capita GDP region. Though the variable of age in model 1 had no effects on probation application, by considering the results of models 2 and 3, and Table V. 4.2-1, the current study found that court location, as an extralegal factor, had a statistically significant effect on the probation application. Neither of the legally relevant factors could predict the probation application.

Hierarchy Linear Regression of Incarceration Length [d]

	Model Summary				Regression ANOVA			Coefficients		
Model	R^2	R^2 ↑	F ↑	p.R^2 ↑	F	P.	Factors	B	*t*	*p.*
1[a]	.074	.074	5.340	.000*	5.340	.000*	(Constants)	4.455	2.604	.010*
							Gender	3.698	3.721	.000*
							Age	.625	1.540	.125
							Education	.733	1.815	.071
							Offender's Region	.041	.156	.876
2[b]	.094	.020	5.804	.017*	5.510	.000*	(Constants)	2.251	1.168	.244
							Gender	3.240	3.321	.001*
							Age	.618	1.534	.126
							Education	.744	1.859	.064
							Offender's Region	.005	.020	.984
							Court Location	.689	2.409	.017*
3[c]	.169	.075	11.983	.000*	7.683	.000*	(Constants)	.007	.004	.997
							Gender	2.918	3.020	.003*
							Age	.727	1.864	.063
							Education	.327	.813	.417
							Offender's Region	-.105	-.412	.680
							Court Location	.677	2.462	.014*
							Crime Conduct	-.115	-.484	.629
							Crime Seriousness	2.423	4.895	.000*

a. Predictors: (Constant), Offender's Region, Gender, Age, Educational Level
b. Predictors: (Constant), Offender's Region, Gender, Age, Educational Level, Court Location
c. Predictors: (Constant), Offender's Region, Gender, Age, Educational Level, Court Location, Crime Seriousness, Crime Conduct
d. Dependent Variable: Incarceration Length
*. $p<0.05$

Table V. 4.3-2 Hierarchy Linear Regression of Incarceration Length

Table V. 4.3-2 provides the results of the hierarchical linear regression of incarceration length. The analytic strategy applied here was the same as in the binary logistic regression. First, in model 1, when putting the offender's characteristics into the model, this study found that: the offender's gender had a significant effect on predicting the sentencing outcome of incarceration length (B=3.698, t=3.721, p=.000). Second, this study added the court location into the model and got model 2. In model 2, this study found that: (1) by adding court location into the model, the change of R^2 was .020, and this change had

statistical significance. It means that the new variable in the model, the court location, could explain more variances; (2) the court location had a significant effect on the prediction of incarceration length (B=.689, *t*=2.409, *p*=.017); and (3) though the court location added into the model and had a significant effect, the effect of the gender had not been dispelled.

Finally, this study added another two variables, the criminal conduct, and the crime seriousness, into the model, i.e., model 3. In model 3, this study found that: (1) by adding two legally relevant factors into the model, the R^2 change was .075 with statistical significance; (2) the crime seriousness had a salient effect on the incarceration length (B=2.423, *t*=4.895, *p*=.000); and (3) the effects of gender and court location had not been dispelled.

Hierarchy Linear Regression of Amounts of Fines [d]

	Model Summary				Regression ANOVA			Coefficients		
Model	R^2	R^2 ↑	F ↑	p.R^2 ↑	F	P.	Factors	B	*t*	*p.*
1[a]	.056	.056	3.964	.004*	3.964	.004*	(Constants)	-.728	-2.624	.009*
							Gender	-.204	-1.267	.206
							Age	.116	1.759	.080
							Education	.149	2.280	.023*
							Region	.057	1.335	.183
2[b]	.056	.000	.070	.791	3.175	.008*	(Constants)	-.768	-2.431	.016*
							Gender	-.212	-1.292	.198
							Age	.116	1.753	.081
							Education	.150	2.279	.023
							Region	.056	1.315	.190
							Court Location	.012	.265	.791
3[c]	.072	.016	.016	.109	2.927	.006*	(Constants)	-.993	-2.967	.003*
							Gender	-.235	-1.430	.154
							Age	.130	1.960	.051
							Education	.110	1.604	.110
							Region	.041	.939	.349
							Court Location	.013	.280	.780
							Crime Conduct	.029	.716	.474
							Crime Seriousness	.160	1.902	.058

a. Predictors: (Constant), Offender's Region, Gender, Age, Educational Level
b. Predictors: (Constant), Offender's Region, Gender, Age, Educational Level, Court Location
c. Predictors: (Constant), Offender's Region, Gender, Age, Educational Level, Court Location, Crime Seriousness, Crime Conduct
d. Dependent Variable: Z-Amounts of Fines
*. *p*<0.05

Table V. 4.3-3 Hierarchy Linear Regression of Amounts of Fines

To sum together, there were four findings in the hierarchical regression of incarceration length: (1) comparing with female offenders, male offenders were sentenced averagely 2.9 months more incarceration. In other words, female offenders would get more

lenient treatment in the sentencing outcomes of incarceration length; (2) the court location played a critical role again in the sentencing outcomes. Offenders who were sentenced in the court of high per capita GDP region were with a higher probability of being sentenced .67 month more incarceration than those in the court of relatively low per capita GDP region; (3) the offenders with high crime seriousness scores were averagely sentenced 2.4 months more than those with low scores; and (4) although the crime seriousness, as a legally relevant factor, had a significant effect on the incarceration length, it could not offset the other two extralegal factors' effects on the sentencing length. The disparities of incarceration length still existed based on extralegal factors.

Table V. 4.3-3 provides the results of the hierarchical linear regression of amounts of fines. Compared with the other two regression results, Table V. 4.3-3 does not too many materials to explain. It is because that, although the three models constructed in the regression of amounts of fines were with statistical significance and the variable of education which had a significant effect on the amounts of fines in model 1, its effects were offset in model 2 and model 3, then made that there were no variables in this study could predict the amounts of fines. The reasons for these results could be: (1) the variables in this study did not correlate with amounts of fines; and (2) the variables in this study might have a correlation with amounts of fines, but because of the small-sized sample, the effects were not significant enough. However, combining with China's judicial practices, a judge could not arbitrarily sentence the offenders' fines; at least the crime seriousness could affect the sentencing outcomes. Then, this result could arguably attribute to the small-sized sample.

5. DISCUSSION AND STAGED SUMMARY

5.1 DISCUSSION

The objective of the current research is to contribute to the sentencing research within the scope of cybercrime. Cybercrime has been a global issue in the recent decade. It is crucial for the general deterrence and prevention of cybercrime whether the sentencing could function well within sentencing guidelines. Because legality is an underlying principle of the sentencing guideline, it is the most important from the perspective of criminal law that the better courts follow the sentencing guideline, the better the fulfillment of the principle of legality is. Though for the consideration of preventing the risks of criminal offenses in modern society, the legislators in China had separated the supportive conducts that aid the commission of a crime from traditional cybercrime and set them as independent auxiliary

cybercrimes. If the legal practitioners, especially the judges, could not sentence the auxiliary cybercriminals closely depend on the sentencing guidelines and criminal law, in other words, depending on the legally relevant factors, then, the function of deterring and preventing related cybercrimes through sentencing and punishments would deviate its original intention or lead to retroactions. In terms of these considerations, the core research questions aimed to explore whether the sentencing disparities within the field of auxiliary cybercrime exist in China, describe whether the extralegal factors cause these disparities, and give an explanation of them, thus offering valuable information for possible sentencing reform.

The main findings could be summarized as follows: incorporating the statistical results of multivariate analyses and regression analyses. First, on the whole, after excluding the effects of crime seriousness as an element of the legally relevant factors of sentencing, the offender's gender and the venue of the case (court location) as the extralegal factors of sentencing could cause the sentencing bias/disparities with statistical significance. The sentencing bias/disparities do exist in sentencing auxiliary cybercriminals in China mainland.

Second, as far as the offender's gender is concerned, its effects on the sentencing outcomes significantly reflected in the incarceration length. Compared with male perpetrators of auxiliary cybercrime, female offenders have a high likelihood of shorter incarceration length. As reported in Table V. 4.3-2, the female would get three months less incarceration length on average than male offenders. This finding is consistent with many valuable pieces of research before.[589] Meanwhile, based on this finding, some critical theoretical articulations could be proven and enriched from there. First, the chivalry perspective contends that the judges in the court, generally, have a paternalistic need to protect female. Thus, female offenders are generally treated more leniently compared to male ones.[590] The thesis of the chivalry complies with the findings in this study. Second, this finding suggests that the focal

[589] e.g., see. PATRICIA L. BRANTINGHAM, 1985, pp. 302-303; KELSEY L. KRAMER AND XIA WANG, 2019, pp. 1303-1307; BARBARA A. KOONS-WITT, ERIC L. SEVIGNY, JOHN D. BURROW AND RHYS HESTER, 2014, pp. 299-324; DARRELL STEFFENSMEIER, NOAH PAINTER-DAVIS AND JEFFERY ULMER, 2017, p. 830; JEFFREY S NOWACKI, 2017, pp. 97-116; KATHLEEN DALY AND REBECCA L. BORDT, 1995, pp. 141-176; GRANT A. BROWN, 2004, pp. 106-108; ILENE H. NAGEL AND JOHN HAGAN, 1983, pp. 91-144; TIMOTHY GRIFFIN AND JOHN WOOLDREDGE, 2006, pp. 893-923; CORTNEY A. FRANKLIN AND NOELLE E. FEARN, 2008, pp. 279-290; DONNA M. BISHOP AND CHARLES E. FRAZIER: The effects of gender on charge reduction. *The Sociological Quarterly*, vol. 25. no. 3. (1984) 385-396; CASSIA C. SPOHN AND JEFFREY W. SPEARS: Gender and Case Processing Decisions: A Comparison of Case Outcomes for Male and Female Defendants Charged with Violent Felonies. *Women & Criminal Justice*, vol. 8. no. 3. (1997) 29-59.

[590] TIMOTHY GRIFFIN AND JOHN WOOLDREDGE, 2006, pp. 893-923; NATALIE GOULETTE, JOHN WOOLDREDGE, JAMES FRANK AND LAWRENCE TRAVIS, 2015, pp. 406-417.

concerns could be applied as a meaningful framework for explaining the gender bias between male and female offenders. Further, female offenders might be treated as less dangerous, risky, and unstable offenders and consequentially less blameworthy for their criminal conduct. Thus, female offenders in the sentencing process are profitably influenced on the individual level, which further causes the sentencing disparities against male ones in the sentencing outcomes.

Third, the court location's effects on the sentencing outcomes are reflected in the incarceration length and probation application. As the regional per capita GDP increases by location, so is the likelihood of probation and shorter incarceration length for auxiliary cybercrime perpetrators decreasing. In other words, looking at the probation application, offenders sentenced in a court located in a higher per capita GDP region are less likely to be put on probation than those sentenced in a court located in a relatively low per capita GDP region. Regarding the incarceration length, offenders who were sentenced in a court located in a higher per capita GDP region were incarcerated for a more extended period than those sentenced in a court located in a relatively low per capita GDP region. This finding was unexpected and surprising. Regional differences in sentencing often occur in connection with crimes where geographic location is the main element of the perpetration, such as human trafficking, drug trafficking[591], and terrorist crimes, yet this is rarely the case with crimes that do not rely heavily on geographic location, such as cybercrime.

Nevertheless, this study attempts to explain this finding with the social world theory and the organizational contexts perspective. First, regarding the social world theory, as mentioned above, criminal courts in different regions could be treated as different social worlds. There is a fundamental activity in each social world, a unique site, and a "technology."[592] Utilizing and explaining the technology (sentencing guideline or criminal law) varies in the different social worlds. In other words, judges in the different regions have a different understanding of the criminal law and the sentencing guideline, thus creating regional disparities within sentencing outcomes. It is reasonable to assume that different regions' higher courts could draft different regional sentencing guidelines based on unique circumstances to the regional socio-environment. Second, concerning the organizational context perspective, which contends that individual sentencing outcomes adjudicated by any criminal court are influenced by the political, social, and organizational context of that court,

[591] PAULA M. KAUTT, 2008, p. 262.
[592] ADELE CLARKE AND SUSAN STAR, 2008, p. 118.

the judges in the different regions would be influenced by the local politics, socio- and organizational context. Combined with the other findings in this study, courts in more developed regions usually make harsher decisions, such as fewer probation sentences and more extended incarceration, than those in less developed regions. It is because the socio- and organizational context varied in different regions. Compared with the low developed region, the more developed region in China has a developed economy and scientific technology, large residents, and large fluid populations. These characteristics create considerable uncertainty for the offenders to re-offend. Therefore, instead of lenient benevolent punishment to bring offenders back to society with the risk of recidivism, the judge might sentence offenders harsher to avoid these uncertainties. It is also in line with the theories of focal concerns and uncertainty avoidance. However, judges' focal concern shifted from the individual level's characteristics to the consideration of the region's socio- and organizational context.

5.2 STAGED SUMMARY

The sentencing disparity is not a new issue, nor is it just a problem with cybercrime sentencing. The legislative and judicial departments of many countries worldwide are reducing unwarranted disparities in sentencing outcomes as much as possible. However, this study believes that reducing the unwarranted disparities in the sentencing outcomes of cybercrime should go faster and further. In this regard, this study attempts to use the rational choice perspective to give reasons.

The rational choice perspective assumes that "decisions about whether (or not) to offend are based on a more or less deliberate calculation on the potential offender's part of the 'risk, rewards and efforts of alternative courses of action.'" "While this does not assume that all such choices are fully rational given constraints of time, ability, and knowledge about the circumstances, it does suggest that offenders are, in effect, constantly ready to take advantage of crime opportunities when they are confronted with them if rational calculation suggests this will be to their advantage."[593]

Cybercrime is not limited by geographic location and has a wide range of impacts and immediacy (short intervals between behavior and benefits, and between behaviors and results). Simultaneously, with the increasing development of information network technology

[593] STEVE CASE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS: *Criminology*. New York, Oxford University Press, 2017.

and people's easier and broader access to the Internet, the threshold for cybercrime has gradually decreased, which is saliently reflected in auxiliary cybercrime. Considering the rational choice perspective, these cybercrime features have already reduced the constraints of time and ability and, to some degree, improved the rewards for the potential offenders. The only factor the potential offenders need to consider is the risk or, better, the expense. However, the unwarranted disparities of the sentencing outcomes caused by extralegal factors would reduce offenders' expense. In this study, they are gender and court location.

First, as for the unwarranted disparities caused by gender, female offenders had a high likelihood of getting more lenient punishments than male ones. It could encourage potential female offenders to commit auxiliary cybercrime more and more. As reported in Table V. 5.2-1, the count of female offenders in this sample revealed an increasing trend by year. Second, in terms of the unwarranted disparities brought with court location, it could have two aspects of effects: (1) it will promote more potential offenders in the less developed region to offend. The count of the auxiliary cybercrime in the less developed region would significantly increase as reported in Table V. 5.2-2 based on the current study's sample; (2) the potential offenders would transfer from the more developed region to less for getting lenient punishment. The remoteness of information technology provides the probability for this approach. To sum, in China's context, the unwarranted disparities in sentencing outcomes of auxiliary cybercrime caused by gender and court location would eliminate the function of crime prevention and deterrence. They could be the perverse incentives to stimulate more potential offenders to offend.

Lessons should be learned from this chapter: As mentioned at the beginning, crime governance is usually inseparable from the two essential steps of conviction and sentencing. Whether the sentencing is fair or not directly affects the effectiveness of crime governance. Through the research in this chapter, we find that even though China's Supreme People's Court has enacted the sentencing guidelines, in judicial practice, especially sentencing practices, the sentencing of cybercrime cases is still affected by extra-legal factors. It could be understood and explained with applications of the chivalry perspective, uncertainty avoidance, the theory of the social world, and the organizational context theory. However, in the whole pursuit of cybercrime governance, sentencing disparities in cybercrime will affect its effectiveness.

Meanwhile, combined with the crime prevention theory and the rational choice theory, this chapter believes that sentencing disparities will further stimulate potential perpetrators to

engage in cybercrime and maximize illegal profits. As part of cybercrime governance in China, the sentencing of cybercrime governance would go against the original intention of cybercrime governance if it indirectly became a criminal inducement. Nevertheless, from the sentencing disparity in cybercrime in China, we can also believe that the shortcomings in sentencing practice in China are the same as those in judicial practice in other countries. It shows that the problem of cybercrime governance, at least in terms of sentencing practices, has global similarities.

Gender Distribution by Year

Count

		Gender		
		Female	Male	Total
Trial Year	2015	0	2	2
	2016	2	9	11
	2017	2	42	44
	2018	24	114	138
	2019	16	62	78
Total		44	229	273

Table V. 5.2-1 Gender Distribution by Year

Offenders Distribution by Court Location*Year

		Court Location				
		1	2	3	4	5
		Count	Count	Count	Count	Count
Trial Year	2015	0	0	2	0	0
	2016	0	0	0	2	9
	2017	0	4	4	3	33
	2018	8	11	40	14	65
	2019	10	7	19	7	35

Table V. 5.2-2 Offenders Distribution by Court Location*Year

VI. CONCLUSIONS

"It was the best of times, it was the worst of times," Charles Dickens wrote at the beginning of his novel *A Tale of Two Cities*. It is a better description of the current world. With the rapid development of information network technology, the world has entered the Internet era. While enjoying the dividend brought by the development of the Internet, human beings are also experiencing the trouble of cybercrime. Global cooperation and establishing a community with a shared future for humankind seem to be the international consensus on cybercrime governance in the current world. As one of the most influential countries globally, China's practice and lessons in cybercrime governance are of great significance to the global governance of cybercrime. This dissertation is based on this cognition. With China's cybercrime governance practice as the core content, it discusses, analyzes, and summarizes the praxis and lessons of China's cybercrime governance practice, hoping to provide Chinese solutions for the global governance of cybercrime.

Chapter II to Chapter V contain the bulk of this doctoral dissertation's content.

In Chapter II - Overview of Cybercrime, this dissertation studies three aspects and draws the following conclusions.

In redefining cybercrime, this article clarifies three commonly used terms: *Computer Crime, High-Technology Crime,* and *Cybercrime*. This dissertation discovers through a study of terminology that:

Computer Crime is concerned with the objectification of cybercrime. It began during the early stages of the development of information network technology, that is, during the era of computers as the central component. However, as technology advances and people use the Internet in a variety of ways, using Computer Crime to represent cybercrime no longer accurately reflects cybercrime's current development characteristics.

At first glance, *High-technology Crime* resembles a description of cybercrime's characteristics. However, the term "High-technology Crime" encompasses a broader range of crimes. High technology does not always imply the use of information networks. As a result, using this term to refer to cybercrime requires further explanation and clarification. At the same time, advanced technology does not necessarily correspond to the characteristics of cybercrime in the modern era:

criminals do not require sophisticated knowledge or technology to commit cybercrime.

Cybercrime is defined as a crime committed in cyberspace. With the advancement of information network technology, it can be said that the distinction between physical and virtual space has always been difficult. With this in mind, cybercrime fairly accurately describes the current state of cybercrime, echoing the global theme of cyberspace governance.

Subsequently, this article redefines cybercrime by fusing relevant criminological theories with the characteristics of cybercrime reflected in the three terms mentioned above. This paper believes that cybercrime is a harmful deviant behavior taken for procuring improper interests forbidden by law and/or common social values, by the feature of the data and online transportation thereof, which abuse the advanced technologies and/or the information asymmetries that get from positional advantages.

In researching the morphology of cybercrime, this dissertation first introduces different theories of the morphological classification of cybercrime. It then discusses the major morphologies of cybercrime in contemporary Chinese criminal law, specifically Chapter VI, Section 1 of the Chinese Criminal Law. This dissertation reveals the following:

There are two primary methods for categorizing cybercrime morphologically in official and academic circles: particularization and generalization. The method of particularization delves into specific cybercrime morphologies as defined by the Budapest Convention of the Council of Europe. The classification system used by the United States Department of Justice summarizes the various types of cybercrime morphologies in general. The majority of academic morphological classifications are based on the generalization method.

Using computers and technology as a reference system, there are three primary morphologies of cybercrime: (1) the computer or computer network is the target of crime; (2) the computer or computer network is a tool to commit a traditional crime; (3) the computer or Internet plays as an incident in committing crimes. This classification is relatively consistent with the official United States taxonomy and reflects an attitude toward cybercrime that places a computer or technology at the center or as a target.

Using criminal behavior as a reference point, cybercrime can be classified into four distinct morphologies: (1) Cyber-theft and deception; (2) Cyber-porn and obscenity; and (3) Cyber-violence. This classification is based on specific criminal law provisions, indicating that some scholars have shifted their focus away from technology and toward behavior.

Using the object of the criminal violation as a reference point, cybercrime can be morphologically classified into four broad categories: (1) cybercrime against the person; (2) cybercrime against property; (3) cybercrime against morality; and (4) cybercrime against the state. This classification focuses on cybercrime's "victims," indicating a shift away from criminal behavior and toward crime outcomes.

China's cybercrime has a morphological structure that is primarily comprised of "*one catch-all clause + eight specific cybercrimes*." The "catch-all clause" reflects the Chinese government's continued belief in cybercrime as an abuse of computer information technology. The "eight specific cybercrimes," which include safeguarding computer information systems, prohibiting the abuse of computer information technology, and defining the criminal responsibilities of accomplices, neutrals, and legal persons in cybercrime, demonstrate that China's criminal law continues to view "technology" as a necessary characteristic of cybercrime.

In applying criminology theory to understand and explain cybercrime, this dissertation relies heavily on the sociological approaches in criminology. By examining strain theory and general strain theory in social structure theory, differential association theory and social learning theory in social process theory, and radical criminology and feminist criminology in social conflict theory, this dissertation establishes the following:

Merton's Strain Theory and Agnew's General Strain Theory belong to the macroscopic theory. They focus on the combination of socio-cultural background and behavioral adaptions of social members to figure out the causes of crime. Using these two theories to understand and explain cybercrime is feasible and profound. However, due to the macroscopic nature of these two theories, it usually takes a long time for social policy adjustment to solve the problems described in these two theoretical frameworks. If these two theories are used to guide the practice of crime governance, they cannot respond to people's demand for cybercrime control in the short term.

Differential Association Theory and Social Learning Theory are micro-level theories. They have an advantage in understanding cybercrime, especially in explaining hacking. However, these two theories also have shortcomings, embodied as follows: first, cyberspace is different from traditional physical space. The social process theory, which is derived from the study of crime in traditional physical space, does not fully consider the uniqueness of cyberspace in the explanation of cybercrime, at least in the existing research of scholars. Second, researchers mostly take students in school as the sample in the current research on explaining cybercrime by using social process theory; the characteristics reflected by the students in school do not have general promotion.

Radical Criminology and Feminist Criminology are reflective theories. Based on social conflicts, they reflect on the causes of a crime arising from social conflicts. In terms of understanding cybercrime, Radical Criminology focuses on whether it is reasonable to criminalize specific behaviors, while Feminist Criminology focuses on protecting the rights of minority groups in particular crimes. This dissertation argues that neither of these theories has practical significance in guiding cybercrime governance. However, it has advantages in understanding the causes of a specific cybercrime.

In the third chapter—China's legislative practice of cyberspace and cybercrime governance, this dissertation mainly introduces and analyzes the legal means system of China's governance of cyberspace and cybercrime from both domestic and international dimensions and draws the following conclusions.

Before discussing and analyzing China's legal means to govern cyberspace and cybercrime, this dissertation briefly introduces the basic characteristics of China's legal system and the source of law. Although Chinese officials and scholars describe China's legal system as a socialist legal system with Chinese characteristics, this dissertation demonstrates that it retains the essential characteristics of the civil law system. The formal source of law in China mainly includes the Constitution, laws formulated by the National People's Congress and its Standing Committee, administrative regulations formulated by the State Council, and departmental rules formulated by constituent departments of the State Council. Informal sources of law in China mainly include policies, guiding cases, and ethnic customs. Judicial

interpretations formulated by the Supreme People's Court and the Supreme People's Procuratorate are not a formal source of law. However, judicial interpretation plays a function similar to laws in China, so this dissertation pays attention to this point in the subsequent research and discusses and analyzes it as a part of the source of Chinese law.

This dissertation mainly introduces China's policies, cyber laws, and cybercriminal law in the domestic dimension of China's legal means system to govern cyberspace and cybercrime.

This dissertation argues that China has established a legal means system to govern cybercrime, "*Guided by the policies of the Communist Party of China + Comprehensive governance of various aspects of society + The bottom means of criminal law*." The legislative practice of cybercrime governance in China shows that: cybercrime governance cannot leave cyberspace governance. Cybercrime governance is a part of cyberspace governance. Cyberspace governance is a systematic social project. Through all-around governance in cyberspace, China regulates deviant Internet activities that do not conform to social values, protects the rights and interests of women and minors, attaches great importance to protecting intellectual property rights, and maintains national cybersecurity and Internet economic development. At the same time, cyberspace governance needs the attention of the state. Cyberspace issues involve all aspects of social development, and it is wise to set up a coordinated and unified department dedicated to cyberspace, such as the Cyberspace Administration of China.

As far as cybercriminal law is concerned, China has continuously revised the Criminal Code through criminal law amendments to adapt to the new situation of cybercrime governance. By analyzing the provisions on cybercrime in China's Criminal Code, this dissertation argues that China's criminal law in cybercrime governance: first is to strengthen the protection of citizens' personal information constantly; the second is to improve the criminal law protection of copyright; the third is criminalizing the assisting behavior and preparation behavior of illegal activities of cybercrime; fourthly, the criminal responsibility of the Internet service providers and online platform operators is stipulated; fifth, China attaches importance to maintaining social order in cyberspace.

The Supreme People's Court and the Supreme People's Procuratorate of China have also supplemented the application of specific provisions of the Criminal Law by constantly formulating judicial interpretations of cybercrime. However, China's judicial interpretation of cybercrime seems too rigid in legislative technology. This dissertation argues that although it is desirable to adopt "qualitative + quantitative" legislative technology to clarify specific crime circumstances, too much emphasis on a quantitative approach will stimulate potential criminals to "reasonably" avoid punishment and thus stimulate the occurrence of cybercrime.

In the international dimension of China's legal means system to govern cyberspace and cybercrime, this dissertation mainly introduces China's participation and role in regional international cooperation in the governance of cyber affairs under the framework of the Shanghai Cooperation Organization.

This dissertation argues that the governance of regional international cooperation in cyber affairs under SCO's framework mainly includes cooperation in cyberspace governance, cooperation in maintaining cybersecurity, and cooperation in combating cybercrime. China has actively participated in regional international cooperation in cyber affairs governance. However, the Shanghai Cooperation Organization with China and Russia as its core has the following problems in the cooperative governance of cyber affairs: First, the cooperation of the Shanghai Cooperation Organization is a mere formality, and much cooperation is embodied in the formulation of regional treaties and the issuance of conference declarations. Second, the SCO cooperation lacks a long-term mechanism, and only one practical exercise has been carried out in some areas of cooperation. The third is the lack of substantive cooperation clauses in the treaties formulated by the SCO to deal with cybercrime. It is more a declaration of political attitude than a legally binding international convention like the Council of Europe's Budapest convention. Accordingly, this paper argues that considering the distinct national conditions of each country, not all regional international cooperation can reach the level of cooperation of European countries. In the long run, establishing a truly feasible global standard is positive for the global governance of cybercrime.

Conviction and sentencing are two critical steps in criminal justice practice. Chapter IV focuses on the conviction practice of Cybercrime governance in China, that is, the

application of criminal law. Chapter V carries out empirical research, focusing on the sentencing practice of cybercrime governance in China.

Chapter IV mainly studies three aspects:

The first is to study China's Internet Real-name system and cybercrime prevention. According to the basic theory of crime prevention, the comprehensive implementation of the Internet Real-name system in China cannot prevent cybercrime well which goes against the original intention of China to establish this system. Meanwhile, the full implementation of the Internet Real-name system can enlarge the harm of cybercrime, restrict citizens' freedom of speech, infringe citizens' privacy, and increase the operating cost of Internet enterprises.

The second is the study of China's governance of online obscene live streaming and the explanation extension of the current criminal law. This dissertation argues that China's current criminal law system is not compatible with the new form of spreading obscenity, such as live streaming; the campaign against pornographic crime cannot leave the support of criminal law. Therefore, the explanation extension of the current criminal law system is an inevitable choice. However, China's legislation and judicial practice in related fields show that China's crackdown on online obscene live streaming violates the principle of legality in criminal law to some extent.

Third, taking the case of DiDi in China as a sample, the dissertation studies the culpable possibilities of online platform operators in the Internet sharing economy. According to the current Criminal Law of China, this dissertation argues that DiDi has management obligations for its online hitch service platform. Furthermore, DiDi should bear criminal responsibility for crimes committed in the hitch service, especially when it fails to fulfill its management obligations faithfully and refuses to correct them after being ordered by the government. Overemphasis on the criminal liability of online platform operators is equivalent to increasing their culpable possibilities. In the short term, it limits the development of online platform operators. In the long run, however, it is conducive to driving the health of the industry.

Chapter IV shows (or Lessons that should be learned from China's practice) that three pairs of relationships should be well handled in cybercrime governance: first, the relationship between Cybercrime Prevention and Human Rights Protection should be well balanced.

Pursuing cybercrime prevention cannot be at the expense of human rights protection. The second is to deal with the relationship between the Principle of Legality in criminal law and the Explanation Extension. In criminal justice, strict adherence to the Principle of Legality in criminal law is not only a requirement of the rule of law but also a guarantee of human rights. To realize cybercrime governance, the Explanation Extension of the current criminal law must follow the Principle of Legality in criminal law. The third is to handle the relationship properly between cybercrime governance and protecting the healthy development of the Internet economy and technology. On the one hand, it can't spare the rat to save the dishes and not interfere with cybercrime caused by the emerging network techniques and economic form. On the other hand, it should keep from going beyond and lead to the development and innovation of new techniques and new economic conditions being limited because of overemphasizing cybercrime governance.

Chapter V conceptualizes Article 287(I) and 287(II) of the Criminal Law of China as the Auxiliary Cybercrime and studies its sentencing disparity.

> The fundamental questions of the research in chapter V include: In the case of the existence of sentencing guidelines in China, is there any disparity in the sentencing of the Auxiliary Cybercrime in judicial practice? If there is sentencing disparity, what are the factors that cause these deviations? Among these factors, which ones are legal factors (those in sentencing guidelines and provisions of the Criminal law) and extralegal factors?
>
> Combined with prior research on sentencing disparity, this dissertation takes focal concern theory, chivalry perspective, and uncertainty avoidance theory as the instruction, through statistical analysis of over 200 Auxiliary Cybercrime judgments, this dissertation found that: although China's courts have sentencing guidelines, there is still sentencing disparity of the Auxiliary Cybercrime. The factors that significantly influence these disparities are the severity of cybercrime cases, the gender of the accused, and the court location. Among them, the seriousness of the crime is the legal factor, while gender and court location are extralegal factors.

The purpose of chapter V is to reflect on and evaluate the sentencing practices of cybercrime governance in China. As mentioned above, the sentencing of cybercrime is an essential aspect of cybercrime governance. Through the empirical analysis in chapter V, this dissertation believes that the sentencing disparity of cybercrime will have a negative impact

on cybercrime governance. It may stimulate the occurrence of cybercrime to some extent and then deviate from the purpose of cybercrime governance. Therefore, to fully realize the goal of cybercrime governance, we must pay attention to the justice of sentencing of cybercrime.

Cybercrime governance is a comprehensive project. Legislation, conviction, and sentencing are all indispensable vital factors therein. In the context of global governance of cybercrime, China's practice and lessons are of reference significance.

APPENDIX I

The Main Currently Effective Administrative Regulations on Cyberspace Governance in China

(*Data Source: Cyberspace Administration of China & PKU LAW Database, up to 2022-03-31*)

1 *Interim Regulations of the People's Republic of China on the Management of International networking of Computer Information*

中华人民共和国计算机信息网络国际联网管理暂行规定

Issuing Authority: State Council

Issuing Date of the latest version: 1997-05-20 Effective Date of the latest version: 1997-05-20

Revision Information: First published on February 1, 1996. Revised on May 20, 1997.

2 *Regulations of the People's Republic of China on Protecting the Safety of Computer Information Systems*

中华人民共和国计算机信息系统安全保护条例

Issuing Authority: State Council

Issuing Date of the latest version: 2011-01-08 Effective Date of the latest version: 2011-01-08

Revision Information: First published on February 18, 1994. Revised on January 8, 2011.

3 *Administrative Measures for the Security Protection of Computer Information Networks Linked to the Internet*

计算机信息网络国际联网安全保护管理办法

Issuing Authority: State Council

Issuing Date of the latest version: 2011-01-08 Effective Date of the latest version: 2011-01-08

Revision Information: First published December 16, 1997. Revised on January 8, 2011.

4 *Administrative Measures for Internet Information Services*

互联网信息服务管理办法

Issuing Authority: State Council

Issuing Date of the latest version: 2011-01-08 Effective Date of the latest version: 2011-01-08

Revision Information: First published September 25, 2000. Revised on January 8, 2011.

5 *Regulation on Computers Software Protection*

计算机软件保护条例

Issuing Authority: State Council

Issuing Date of the latest version: 2013-01-30 Effective Date of the latest version: 2013-03-01

Revision Information: First published on December 20, 2001. First revised on January 8, 2011. Second revised on January 30, 2013.

6 *Regulation on the Protection of the Right to Communicate Works to the Public over Information Networks*

信息网络传播权保护条例

Issuing Authority: State Council

Issuing Date of the latest version: 2013-01-30 Effective Date of the latest version: 2013-03-01

Revision Information: First published on May 18, 2006. Revised on January 30, 2013.

7 *Telecommunication Regulation of the People's Republic of China*

中华人民共和国电信条例

Issuing Authority: State Council

Issuing Date of the latest version: 2016-02-06 Effective Date of the latest version: 2016-02-06

Revision Information: First published on September 25, 2000. First revised on July 29, 2014. Second revised on February 6, 2016.

8 *Provisions on the Administration of Foreign-funded Telecommunications Enterprises*

外商投资电信企业管理规定

Issuing Authority: State Council

Issuing Date of the latest version: 2016-02-06 Effective Date of the latest version: 2016-02-06

Revision Information: First published on December 11, 2001. First revised on September 10, 2008. Second revised on February 6, 2016.

9 *Regulations on the Administration of Business Premises of Internet Access Service*

互联网上网服务营业场所管理条例

Issuing Authority: State Council

Issuing Date of the latest version: 2019-03-24 Effective Date of the latest version: 2019-03-24

Revision Information: First published on September 29, 2002. First revised on January 8, 2011. Second revised on February 6, 2016. Third revised on March 24, 2019.

10 *Regulation on Protecting the Security of Critical Information Infrastructure*

关键信息基础设施安全保护条例

Issuing Authority: State Council

Issuing Date of the latest version: 2021-07-30 Effective Date of the latest version: 2021-09-01

Revision Information: N/A

APPENDIX II

The Main Currently Effective Departmental Rules on Cyberspace Governance in China

(*Data Source: Cyberspace Administration of China & PKU LAW Database, up to 2022-03-31*)

1 *Provisions on Administration of Provision of Financial Information Services in China by Foreign Institutions*

外国机构在中国境内提供金融信息服务管理规定

Issuing Authority: State Council Information Office
Ministry of Commerce
State Administration for Industry & Commerce (dissolved)

Issuing Date of the latest version: 2009-04-30 Effective Date of the latest version: 2009-06-01

2 *Several Provisions on Regulating the Market Order of Internet Information Services*

规范互联网信息服务市场秩序若干规定

Issuing Authority: Ministry of Industry & Information Technology

Issuing Date of the latest version: 2011-12-29 Effective Date of the latest version: 2012-03-15

3 *Provisions on Protecting the Personal Information of Telecommunications and Internet Users*

电信和互联网用户个人信息保护规定

Issuing Authority: Ministry of Industry & Information Technology

Issuing Date of the latest version: 2013-07-16 Effective Date of the latest version: 2013-09-01

4 *Provisions on the Administration of Internet Audio-Visual Program Service*

互联网视听节目服务管理规定

Issuing Authority: State Administration of Press, Publication, Radio, Film & Television (dissolved)

Issuing Date of the latest version: 2015-08-28 Effective Date of the latest version: 2015-08-28

Revision Information: First published December 20, 2007. Revised on August 28, 2015.

5 *Provisions on the Administration of Online Publishing Services*

网络出版服务管理规定

Issuing Authority: State Administration of Press, Publication, Radio, Film & Television (dissolved)
Ministry of Industry & Information Technology

Issuing Date of the latest version: 2016-02-04 Effective Date of the latest version: 2016-03-10

6 *Provisions on the Administrative Law Enforcement Procedures for Internet Information Content Management*

互联网信息内容管理行政执法程序规定

Issuing Authority: Cyberspace Administration of China

Issuing Date of the latest version: 2017-05-02 Effective Date of the latest version: 2017-06-01

7 *Provisions for the Administration of Internet News Information Services*

互联网新闻信息服务管理规定

Issuing Authority: Cyberspace Administration of China

Issuing Date of the latest version: 2017-05-02 Effective Date of the latest version: 2017-06-01

8 *Measures for the Administration of Internet Domain Names*

互联网域名管理办法

Issuing Authority: Ministry of Industry & Information Technology

Issuing Date of the latest version: 2017-08-24 Effective Date of the latest version: 2017-11-01

9 *Interim Provisions on the Administration of Internet Culture*

互联网文化管理暂行规定

Issuing Authority: Ministry of Culture (dissolved)

Issuing Date of the latest version: 2017-12-15 Effective Date of the latest version: 2017-12-15

Revision Information: First published on May 10, 2003. Republished on February 17, 2011. Revised on December 15, 2017.

10 *Provisions on the Administration of Blockchain Information Services*

区块链信息服务管理规定

Issuing Authority: Cyberspace Administration of China

Issuing Date of the latest version: 2019-01-10 Effective Date of the latest version: 2019-02-15

11 *Provisions on the Cyber Protection of Children's Personal Information*

儿童个人信息网络保护规定

Issuing Authority: Cyberspace Administration of China

Issuing Date of the latest version: 2019-08-22 Effective Date of the latest version: 2019-10-01

12 *Provisions on Ecological Governance of Network Information Content*

网络信息内容生态治理规定

Issuing Authority: Cyberspace Administration of China

Issuing Date of the latest version: 2019-12-15 Effective Date of the latest version: 2020-03-01

13 *Provisions on the Administration of Private Network and Targeted Communication Audiovisual Program Services*

专网及定向传播视听节目服务管理规定

Issuing Authority: National Radio & Television Administration

Issuing Date of the latest version: 2021-03-23 Effective Date of the latest version: 2021-03-23

Revision Information: First published April 25, 2016. Revised on March 23, 2021.

14 *Several Provisions on the Management of Automobile Data Security (for Trial Implementation)*

汽车数据安全管理若干规定（试行）

Issuing Authority: Cyberspace Administration of China
State Development & Reform Commission
Ministry of Industry & Information Technology
Ministry of Public Security
Ministry of Transport

Issuing Date of the latest version: 2021-08-16 Effective Date of the latest version: 2021-10-01

15 *Measures for Cybersecurity Review*

网络安全审查办法

Issuing Authority: Cyberspace Administration of China
State Development & Reform Commission
Ministry of Industry & Information Technology
Ministry of Public Security
Ministry of State Security
Ministry of Finance
Ministry of Commerce
People's Bank of China
State Administration for Market Regulation
National Radio & Television Administration
China Securities Regulatory Commission
State Secrets Bureau
State Encryption Administration

Issuing Date of the latest version: 2021-12-28 Effective Date of the latest version: 2022-02-15

16 *Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services*

互联网信息服务算法推荐管理规定

Issuing Authority: Cyberspace Administration of China
Ministry of Industry & Information Technology
Ministry of Public Security
State Administration for Market Regulation

Issuing Date of the latest version: 2021-12-31 Effective Date of the latest version: 2022-03-01

APPENDIX III

The Main Currently Effective Judicial Interpretations on Cybercrime in China

(*Data Source: PKU LAW Database, up to 2021-07-31*)

1 *Interpretation on Several Issues concerning the Concrete Application of Law in the Handling of Criminal Cases of Making, Reproducing, Publishing, Selling and Spreading Pornographic Electronic Information by Means of the Internet, Terminal of Mobile Communications and Sound Message Stations*
关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2004-09-06

2 *Interpretation (II) of Several Issues on the Specific Application of Law in the Handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Disseminating Pornographic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations*
关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2010-02-04

3 *Interpretation of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems*
关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2011-09-01

4 *Interpretation on Several Issues concerning the Specific Application of Law in the Handling of Defamation through Information Networks and Other Criminal Cases*
关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2013-09-10

5 *Opinions on Several Issues Concerning the Application of Law in the Handling of Telecommunications Network Fraud and other Criminal Cases*
关于办理电信网络诈骗等刑事案件适用法律若干问题的意见

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate
Ministry of Public Security

Effectiveness: Effective Effective Date: 2016-12-20

6 *Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information*

关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2017-06-01

7 *Minutes of the Symposiums on Issues concerning Handling Internet-related Financial Crime Cases*

关于办理涉互联网金融犯罪案件有关问题座谈会纪要

Issuing Authority: Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2017-06-02

8 *Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases regarding Organizing, Forcing, Inducing, Sheltering, or Introducing Prostitution*

关于办理组织、强迫、引诱、容留、介绍卖淫刑事案件适用法律若干问题的解释

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2017-07-25

9 *Official Reply on Issues concerning Conviction and Sentencing for Activities of Profit-Making through Production, Reproduction, Selling, and Dissemination of Pornographic Electronic Information by Using Cloud Storage*

关于利用网络云盘制作、复制、贩卖、传播淫秽电子信息牟利行为定罪量刑问题的批复

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2017-12-01

10 *Guidelines for the Procuratorial Organs in Handling Cases Involving Infringement of Citizens' Personal Information*

检察机关办理侵犯公民个人信息案件指引

Issuing Authority: Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2018-11-09

11 *Guidelines for the Procuratorial Organs in Handling Telecom and Network Fraud Cases*

检察机关办理电信网络诈骗案件指引

Issuing Authority: Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2018-11-09

12 *Opinions on Several Issues of Handling Criminal Cases Involving Gangland Crimes Committed by Using Information Network*

关于办理利用信息网络实施黑恶势力犯罪刑事案件若干问题的意见

Issuing Authority: Supreme People's Court
Supreme People's Procuratorate
Ministry of Public Security

Ministry of Justice

Effectiveness: Effective Effective Date: 2019-10-21

13 *Interpretations on Several Issues concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to Information Network*

关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释

Issuing Authority: Supreme People's Court

Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2019-11-01

14 *Opinions on Punishing Criminal and Illegal Activities that Hinder the Prevention and Control of Novel Coronavirus Pneumonia*

关于依法惩治妨害新型冠状病毒感染肺炎疫情防控违法犯罪的意见

Issuing Authority: Supreme People's Court

Supreme People's Procuratorate

Ministry of Public Security

Ministry of Justice

Effectiveness: Effective Effective Date: 2020-02-06

15 *Provisions on the Handling of Cybercrime Cases by People's Procuratorates*

人民检察院办理网络犯罪案件规定

Issuing Authority: Supreme People's Procuratorate

Effectiveness: Effective Effective Date: 2021-01-22

16 *Opinions on Several Issues Concerning the Application of Law in the Handling of Telecommunications Network Fraud and other Criminal Cases (II)*

关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）

Issuing Authority: Supreme People's Court

Supreme People's Procuratorate

Ministry of Public Security

Effectiveness: Effective Effective Date: 2021-07-17

BIBLIOGRAPHY

Books

[1] ADLER, ALFRED: What Life Could Mean to You. Business and Leadership Publishing, 2014.

[2] AGNEW, ROBERT: Why do Criminals Offend: A General Theory of Crime and Delinquency. New York, Oxford University Press, 2005.

[3] AGNEW, ROBERT: Pressured into Crime: An Overview of General Strain Theory. New York, Oxford University Press, 2006.

[4] AKERS, RONALD L.: Deviant Behavior: A Social Learning Approach. Belmont, California, Wadsworth, 1973.

[5] AKERS, RONALD L.: Social Learning and Social Structure: A General Theory of Crime and Deviance. New York, Routledge, 2009.

[6] ANDERSON, CRAIG A., DOUGLAS A. GENTILE AND KATHERINE E. BUCKLEY: Violent Video Game Effects on Children and Adolescents: Theory, Research, and Public Policy. New York, Oxford University Press, 2007.

[7] BAI, JIANJUN: Empirical Criminal Law and Sentencing Practice: Big Sample Perspective on Criminal Law Phenomena [刑法规律与量刑实践: 刑法现象的大样本考察]. Beijing, Peking University Press, 2011.

[8] BENTHAM, JEREMY: Theory of Legislation. London, Trübner & Company, 1871.

[9] BOOT, MACHTELD: Genocide, Crimes Against Humanity, War Crimes: Nullum Crimen Sine Lege and the Subject Matter Jurisdiction of the International Criminal Court. Antwerpen, New York, Intersentia, 2002.

[10] BRENNER, SUSAN W.: Cybercrime and the Law: Challenges, Issues, and Outcomes. Boston, Northeast University Press, 2012.

[11] CASE, STEVE, PHIL JOHNSON, DAVID MANLOW, ROGER SMITH AND KATE WILLIAMS: Criminology. New York, Oxford University Press, 2017.

[12] CASEY, EOGHAN: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. New York, Academic Press, 2000.

[13] CHARON, JOEL M.: Symbolic Interactionism: An Introduction, An Interpretation, An Integration. United States, Pearson, 2010. 10th Edition

[14] CHESNEY-LIND, MEDA AND LISA PASKO: The Female Offender: Girls, Women, and Crime. Thousand Oaks, California, Sage, 2013.

[15] CHINESE SOCIETY OF CRIMINOLOGY: Annual Research Report on Crime Trends (2018). Beijing, Law Press China, 2019.

[16] CLOWARD, RICHARD A. AND LLOYD E. OHLIN: Delinquency and Opportunity. Chicago, Illinois, University of Chicago Press, 1960.

[17] COHEN, STANLEY: Folk Devils and Moral Panics: The Creation of the Mods and Rockers. London, Routledge, 2011.

[18] CRAIG, BRAIN: Cyberlaw: The Law of the Internet and Information Technology. United States, Pearson, 2012.

[19] CRAWFORD, ADAM: Crime Prevention and Community Safety. London, Longman, 1998.

[20] CROALL, HAZELL: Understanding White Collar Crime. Buckingham, United Kingdom, Open University Press, 2001.

[21] DAVID, RENÉ AND JOHN E. C. BRIERLEY: Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law. New York, The Free Press, 1978.

[22] DUFF, R. A.: Answering for Crime: Responsibility and Liability in the Criminal Law. Oxford, Hart Publishing, 2007.

[23] DUGGAL, PAVAN: Artificial Intelligence, Cybercrimes & Cyberlaw. Independently Published, 2018.

[24] DUGGAL, PAVAN: Cyber Sovereignty & Cyberlaw. Independently Published, 2018.

[25] DUNNE, ROBERT: Computers and the Law: An Introduction to Basic Legal Principles and their Applications in Cyberspace. New York, Cambridge University Press, 2009.

[26] DURKHEIM, ÉMILE: Suicide: A Study in Sociology. London, Routledge, 1951. 2nd Edition

[27] DURKHEIM, ÉMILE: The Rules of Sociological Method. New York, The Free Press, 1982. 1st American Edition

[28] DURKHEIM, ÉMILE: The Division of Labor in Society. New York, The Free Press, 2014.

[29] EDITORIAL, CRIMINAL LAW: Criminal Law (Volume1: General) [刑法学（上册・总论）]. Beijing, Higher Education Press, 2019.

[30] FURNELL, STEVEN: Cybercrime: Vandalizing the Information Society. London, Addison-Wesley, 2001.

[31] GAO, MINGXUAN AND KECHANG MA: Criminal Law [刑法学]. Beijing, Peking University Press, 2022. 10th Edition

[32] GAROFALO, BARON RAFFAELE: Criminology. Boston, Little, Brown, and Company, 1914.

[33] GOTTFREDSON, MICHAEL R. AND TRAVIS HIRSCHI: A General Theory of Crime. Stanford, California, Stanford University Press, 1990. 297.

[34] GROSSMANN, MATT: Artists of the Possible: Governing Networks and American Policy Change since 1945. New York, Oxford University Press, 2014.

[35] HALLEVY, GABRIEL: A Modern Treatise on the Principle of Legality in Criminal Law. Heidelberg, Springer, 2010.

[36] HIGGINS, GEORGE E.: Cybercrime: An Introduction to an Emerging Phenomenon. New York, McGraw-Hill, 2010.

[37] HILL, JOSHUA B. AND NANCY E. MARION: Introduction to Cybercrime: Computer Crimes, Laws,

and Policing in the 21st Century. California, Praeger: ABC-CLIO, LLC, 2016.

[38] HINDUJA, SAMEER: Music Piracy and Crime Theory. New York, LFB Scholarly Publishing, 2006.

[39] HINDUJA, SAMEER AND JUSTIN W. PATCHIN: Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. California, Corwin, 2015. 2nd Edition

[40] HIRSCHI, TRAVIS: Causes of Delinquency. New York, Routledge, 2002.

[41] HOLT, THOMAS J. AND ADAM M. BOSSLER: Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. London and New York, Routledge, 2016.

[42] JENKINS, PHILIP: Beyond Tolerance: Child Pornography on the Internet. New York, New York University Press, 2001.

[43] JI, WEIMIN, JIE SHEN, BINYAN YANG AND LIN JI: Annual report on the Internet use and reading practice of Chinese minors [中国未成年人互联网运用和阅读实践报告 (2017～2018)]. Beijing, Social Science Academic Press (China), 2018.

[44] JORDAN, TIM AND PAUL A. TAYLOR: Hacktivism and Cyberwars: Rebels with a Cause? London, Routledge, 2004.

[45] KEITH, RONALD C.: China's Struggle for the Rule of Law. London, Palgrave Macmillan UK, 1994.

[46] KITTICHAISAREE, KRIANGSAK: Public International Law of Cyberspace. Swizerland, Spinger, 2017.

[47] KOVACICH, GERALD L AND WILLIAM C BONI: High-technology crime investigator's handbook: establishing and managing a high-technology crime prevention program. Elsevier, 2011.

[48] KOVACICH, GERALD L. AND ANDY JONES: High-Technology Crime Investigator's Handbook: Establishing and Managing a High-Technology Crime Prevention Program. Oxford, Elsevier, 2006. 2nd Edition

[49] KREMLING, JANINE AND AMANDA M. SHARP PAKER: Cyberspace, Cybersecurity, and Cybercrime. SAGE Publications, 2017.

[50] LANE, FREDERICK: Obscene Profits: Entrepreneurs of Pornography in the Cyber Age. New York, Routledge, 2001.

[51] LEVY, STEVEN: Hackers: Heroes of the computer revolution. New York, Anchor Press/Doubleday, 1984.

[52] LI, WEI: Fundamental Categories of Criminology [犯罪学的基本范畴]. Beijing, Peking University Press, 2004.

[53] LILLEY, PETER: Hacked, Attacked and Abused: Digital Crime Exposed London, Kogan Page Business Books, 2003.

[54] LU, SHUHUA: Social Statistics [社会统计学]. Beijing, Peking University Press, 2009. 4th Edition

[55] MALBY, STEVEN, ROBYN MACE, ANIKA HOLTERHOF, CAMERON BROWN, STEFAN KASCHERUS AND EVA IGNATUSCHTSCHENKO(UNODC): Comprehensive Study on Cybercrime (Draft). Vienna, United Nations Office on Drugs and Crime, 2013.

[56] MEI, JIE: Criminal Regulations on Web Live Video Streaming [网络直播的刑法规制]. Harbin, China, Heilongjiang University, 2017.

[57] MENDEL, TOBY, ANDREW PUDDEPHATT, BEN WAGNER, DIXIE HAWTIN AND NATALIA TORRES: Global survey on internet privacy and freedom of expression. Paris, United Nations Educational, Scientific and Cultural Organization (UNESCO), 2012.

[58] MERTON, ROBERT K.: Social Theory and Social Structure. Glencoe, Illinois, The Free Press, 1957.

[59] MERTON, ROBERT K.: Social Theory and Social Structure. New York, The Free Press, 1968.

[60] MESSERSCHMIDT, JAMES W.: Capitalism, Patriarchy, and Crime: Toward a Socialist Feminist Criminology. Totowa, New Jersey, Roman and Littlefield, 1986.

[61] MESSERSCHMIDT, JAMES W: Masculinities and Crime: Critique and Reconceptualization of Theory. Lanham, Maryland, Rowman & Littlefield, 1993.

[62] MESSNER, STEVEN F. AND RICHARD ROSENFELD: Crime and the American Dream. Belmont, California, Wadsworth, 2013. 5th Edition

[63] MOORE, ROBERT: Cybercrime: Investigating High-technology Computer Crime. Oxford and New York, Routledge, 2015. 2nd Edition

[64] NETTLER, GWYNN: Explaining Crime. New York, McGraw-Hill, 1974.

[65] PELFREY, WILLIAM V.: The Evolution of Criminology. Cincinnati, Ohio, Anderson, 1980.

[66] PFOHL, STEPHEN: Images of Deviance and Social Control: A Sociological History. New York, McGraw-Hil, 1994.

[67] POST, DAVID G.: In Search of Jefferson's Moose: Notes on the State of Cyberspace. New York, Oxford University Press, 2009.

[68] POTTER, PITMAN B.: The Chinese Legal System: Globalization and Local Legal Culture. London, Routledge, 2001.

[69] QUINNEY, RICHARD: Bearing Witness to Crime and Social Justice. Albany, State University of New York Press, 2000.

[70] REDISH, MARTIN H.: The Adversary First Amendment: Free Expression and the Foundations of American Democracy. Stanford, Stanford University Press, 2013.

[71] ROSENOER, JONATHAN: CyberLaw: The Law of the Internet. New York, Springer, 1997.

[72] ROXIN, CLAUS: Kriminalpolitik und Strafrechtssystem. Berlin/Boston, De Gruyter, 1973.

[73] SCHMITT, MICHAEL N. AND LILS VIHUL: Tallinn manual 2.0 on the international law applicable to cyber operations / Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. New York, Cambridge University Press, 2017.

[74] SHECAIRA, FÁBIO P.: Legal Scholarship as a Source of Law. New York, Springer, 2013.

[75] SHU, GUOYING: Introduction to Jurisprudence [法理学导论]. Beijing, Peking University Press, 2019. 3rd Edition

[76] SIEGEL, LARRY J.: Criminology: Theories, Patterns, and Typologies. Boston, Massachusetts,

CENGAGE Learning, 2016. 13th Edition

[77] SKINNER, BURRHUS F.: Science and human behavior. Oxford, England, Macmillan, 1953.

[78] SMART, CAROL: Women, Crime, and Criminology: A Feminist Critique. London, Routledge, 1976.

[79] STEINMETZ, KEVIN F. AND MATT R. NOBLES: Technocrime and Criminological Theory. New York, Routledge, 2018.

[80] SUNSTEIN, CASS R.: Infotopia: How Many Minds Produce Knowledge. New York, Oxford University Press, 2006.

[81] SUTHERLAND, EDWIN H., DONALD R. CRESSEY AND DAVID F. LUCKENBILL: Principles of Criminology. Lanham, Maryland, General Hall 1992. 11th Edition

[82] TEMKIN, JENNIFER AND BARBARA KRAHÉ: Sexual Assault and the Justice Gap: A Question of Attitude. Oxford, Hart Publishing, 2008.

[83] TENG, YUN: The Criminal Law Analysis of Internet Pornographic Broadcast [网络色情直播行为的刑法分析]. Lanzhou, China, Lanzhou University, 2018.

[84] VOLD, GEORGE B.: Theoretical criminology. Oxford, England, Oxford Univer. Press, 1958.

[85] WALL, DAVID S.: Cybercrime: The Transformation of Crime in the Information Age. Cambridge, Polity, 2007.

[86] WARR, MARK: Companions in Crime: The Social Aspects of Criminal Conduct. New York, Cambridge University Press, 2002.

[87] WIENER, NORBERT: Cybernetics: Or Control and Communication in the Animal and the Machine. New York, Jonh Wiley & Sons, 1948.

[88] WILKINS, LESLIE: Social Deviance. London, Tavistock, 1964.

[89] WILSON, DAVID AND SEAN O'SULLIVAN: Images of Incarceration: Representations of Prison in Film and Television Drama. Winchester, Waterside Press, 2004.

[90] WU, XIAOMEI: Law Yearbook of China-2018. Beijing, Press of Law Yearbook of China, 2018.

[91] WU, ZONGXIAN: History of Criminology in the West [西方犯罪学史]. Beijing, Press of People's Public Security University of China, 2010. 2nd Edition

[92] YAR, MAJID: Cybercrime and Society. New Delhi, Sage, 2013. 2nd Edition

[93] YAR, MAJID AND KEVIN F. STEINMETZ: Cybercrime and Society. London, Sage, 2019. 3rd Edition

[94] YEN, CHING-YUEH: Crime in relations to Social Change in China [中国的犯罪问题与社会变迁的关系]. Beijing, The Commercial Press, 2019.

[95] YU, BOYA: A Qualitative Research on Related Offences of Obscene Live Streaming [互联网淫秽直播相关行为定性研究]. Wuhan, China, Wuhan University, 2022.

[96] ZHANG, MINGKAI: Essentials of Foreign Criminal Law [外国刑法纲要]. Beijing, Law Press, 2020. 3rd Edition

[97] ZHANG, MINGKAI: Criminal Law [刑法学]. Beijing, Law Press, 2021. 6th Edition

[98] ZHANG, WENXIAN: Jurisprudence [法理学]. Beijing, Peking University Press & Higher Education Press, 2011. 4th Edition

[99] ZHANG, WENXIAN: Jurisprudence [法理学]. Beijing, Higher Education Press, 2018. 5th Edition

[100] ZHANG, XIAOHU: Criminology [犯罪学]. Beijing, China Renmin University Press, 2017. 2nd Edition

[101] ZHANG, YUANHUANG: Criminology [犯罪学]. Beijing, China Renmin University Press, 2020. 4th Edition

[102] ZHAO, MOLIN: The Legal Regulations on the Webcast [网络直播的法律规制]. Changchun, China, Jilin University, 2017.

Book Sections

[103] BANDURA, ALBERT: Modeling Theory: Some Traditions, Trends, and Disputes. In: ROSS D. PARKE (ed): *Recent Trends in Social Learning Theory*. Academic Press, 1972. 35-61.

[104] BANKS, JAMES: Radical Criminology and the Techno-Security-Capitalist Complex. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 103-119.

[105] BOMAN, JOHN H. IV AND ADRIENNE FRENG: Differential Association Theory, Social Learning Theory, and Technocrime. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 72-82.

[106] BRENNER, SUSAN W.: Defining Cybercrime: A review of federal and state law. In: RALPH D. CLIFFORD (eds): *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*. Raleigh, Carolina Academic Press, 2011. 15-104.

[107] BURMAN, MICHELE AND LORAINE GELSTHORPE: Feminist Criminology: Inequalities, Powerlessness, and Justice. In: ALISON LIEBLING, SHADD MARUNA AND LESLEY MCARA (eds): *The Oxford Handbook of Criminology*. Oxford, Oxford University Press, 2017. 213-238.

[108] CHISM, KIMBERLY A. AND KEVIN F. STEINMETZ: Technocrime and Strain Theory. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 83-101.

[109] CLARKE, RONALD V. AND KATE BOWERS: Seven Misconceptions of Situational Crime Prevention. In: NIKE TILLEY AND AIDEN SIDEBOTTOM (eds): *Handbook of Crime Prevention and Community Safety*. New York, Routledge, 2017. 109-142.

[110] CRAWFORD, ADAM AND KAREN EVANS: Crime Prevention and Community Safety. In: ALISON LIEBLING, SHADD MARUNA AND LESLEY MCARA (eds): *The Oxford Handbook of Criminology* Oxford, Oxford University Press, 2017. 797-824.

[111] CULLEN, FRANCIS T., MICHAEL L. BENSON AND MATTHEW D. MAKARIOS: Developmental and Life-Course Theories of Offending. In: BRANDON C. WELSH AND DAVID P. FARRINGTON (eds):

The Oxford Handbook of Crime Prevention. Oxford, Oxford University Press, 2012. 23-45.

[112] FRIEDRICHS, DAVID O.: Radical Criminology in the United States: An Interpretive Understanding. In: JAMES A. INCIARDI (ed): *Radical Criminology: The Coming Crises*. Beverly Hills, California, Sage, 1980. 35-60.

[113] GRABOSKY, PETER N.: Unintended Consequences of Crime Prevention. In: ROSS HOMEL (ed): *The Politics and Practice of Situational Crime Prevention*. New York, Criminal Justice Press, 1996. 25-56.

[114] GREER, C. AND R. REINER: Mediated Mayhem: Media, Crime, and Criminal Justice. In: M. MAGUIRE, R. MORGAN AND R. REINNER (eds): *The Oxford Handbook of Criminology*. Oxford, Oxford University Press, 2015. 255-256.

[115] HEIDENSOHN, FRANCES AND MARISA SILVESTRI: Gender and Crime. In: MIKE MAGUIRE, ROD MORGAN AND ROBERT REINER (eds): *The Oxford Handbook of Criminology*. Oxford, Oxford University Press, 2012. 336-369.

[116] KOOPS, BERT-JAAP: Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. In: BABAK AKHGAR AND BEN BREWSTER (eds): *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Switzerland, Springer, 2016. 3-16.

[117] LEMAN-LANGLOIS, STEPHANE: Introduction: Technocrime. In: STEPHANE LEMAN-LANGLOIS (ed): *Technocrime: Technology, Crime, and Social Control*. Devon, UK, Willan Publishing, 2008. 1-13.

[118] MARGANSKI, ALISON J.: Feminist Theory and Technocrime: Examining Gender Violence in Contemporary Society. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 28-51.

[119] MERTON, ROBERT K: Anomie, Anomia, and Social Interaction: Contexts of Deviant Behavior. In: MARSHALL B. CLINARD (eds): *Anomie and Deviant Behavior: A Discussion and Critique*. Toronto, Ontario, The Free Press, 1964. 213-242.

[120] MORRIS, ROBERT G.: Computer Hacking and the Techniques of Neutralization: An Empirical Assessment. In: THOMAS J. HOLT AND BERNADETTE H. SCHELL (eds): *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Hershey, PA, USA, IGI Global, 2011. 1-17.

[121] NATIONAL BUREAU OF STATISTICS OF CHINA: Gross Regional Product (2018). In: SHENGYONG MAO AND ZHICAI YE (eds): *China Statistical Yearbook-2019*. Beijing, China Statistics Press, 2019.

[122] PHILPOT, DUNCAN: Symbolic Interactionism and Technocrime: SWATing as Episodic and Agentic. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 102-118.

[123] REED, CHRIS: Introduction. In: CHRIS REED (ed): *Computer Law*. Oxford University Press, 2011. IV-IVIII.

[124] REINER, ROBERT: Media Made Criminality. In: M. MAGUIRE, R. MORGAN AND R. REINER (eds):

The Oxford Handbook of Criminology. Oxford, Oxford University Press, 1997. 376-377.

[125] REYNS, BRADFORD W.: Routine Activity Theory and Cybercrime: A Theoretical Appraisal and Literature Review. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 52-71.

[126] SELLERS, BRIAN G. AND BRUCE A. ARRIGO: Postmodern Criminology and Technocrime. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 150-163.

[127] SHOVER, NEAL AND JENNIFER SCROGGINS: Organizational Crime. In: MICHAEL TONRY (ed): *The Oxford Handbook of Crime and Public Policy*. Oxford University Press, 2011.

[128] SMITH, MARTHA J. AND RONALD V. CLARKE: Situational Crime Prevention: Classifying Techniques Using "Good Enough" Theory. In: BRADON C. WELSH AND DAVID P. FARRINGTON (eds): *The Oxford Handbook of Crime Prevention*. Oxford, Oxford University Press, 2012. 291-315.

[129] STEFFENSMEIER, DARRELL AND NOAH PAINTER-DAVIS: Focal Concerns Theory as Conceptual Tool for Studying Intersectionality in Sentencing Disparities: Focus on Gender and Race Along With Age. In: JEFFERY T. ULMER AND MINDY S. BRADLEY (eds): *Handbook on Punishment Decisions: Locations of Disparity*. New York, Routledge, 2017. 189-210.

[130] STEINMETZ, KEVIN F. AND MATT R. NOBLES: Introduction. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 1-10.

[131] TILLEY, NICK: Crime Prevention in Britain, 1975-2010: Breaking Out, Breaking In, and Breaking Down. In: GORDON HUGHES, EUGENE MCLAUGHLIN AND JOHN MUNCIE (eds): *Crime Prevention and Community Safety: New Directions*. London, Sage, 2002. 12-36.

[132] TYLOR, EDWARD BURNETT: The Science of Culture. In: EDWARD BURNETT TYLOR (eds): *Primitive Culture: Researches into the Development of Mythology, Philosophy, Religion, Art, and Custom*. Cambridge, Cambridge University Press, 2010. 1-22.

[133] WALL, DAVID S.: Crime and the Internet. In: DAVID S. WALL (eds): *Crime and the Internet*. London, Routledge, 2001. 1-17.

[134] WALL, DAVID S.: The Internet a Conduit for Criminal Activity. In: APRIL PATTAVINA (ed): *Information Technology and The Criminal Justice System*. Thousand Oaks, California, Sage, 2005. 77-98.

[135] WELSH, BRANDON C. AND DAVID P. FARRINGTON: Crime Prevention and Public Policy. In: BRANDON C. WELSH AND DAVID P. FARRINGTON (eds): *The Oxford Handbook of Crime Prevention*. Oxford, Oxford University Press, 2012. 3-22.

[136] WESTMARLAND, NICOLE: Still Little Justice for Rape Victim Survivors: The Void between Policy and Practice in England and Wales. In: NICOLE WESTMARLAND AND GEETANJALI GANGOLI (eds): *International Approaches to Rape*. Bristol, The Policy Press, 2011. 79-100.

[137] YAR, MAJID: Computer Crime Control as Industry: Virtual Insecurity and the Market for Private

Policing. In: KATJA FRANKO AAS, HELENE OPPEN GUNDHUS AND HEIDI MORK LOMELL (eds): *Technologies of InSecurity: The Surveillance of Everyday Life*. London, Routledge-Cavendish, 2008. 189-204.

[138] YAR, MAJID: Toward a Cultural Criminology of the Internet. In: KEVIN F. STEINMETZ AND MATT R. NOBLES (eds): *Technocrime and Criminological Theory*. New York, Routledge, 2018. 133-149.

Conference Papers

[139] AURONEN, LAURI: Asymmetric information: theory and applications. Tu-91.167 Seminar of Strategy and International Business Helsinki University of Technology, Citeseer, 2003. 1-35.

[140] WU, YUQIANG: The Qualitative Analysis of the Behavior of Network "Crossing-The-Wall" Tools in Illegal Sales [非法销售网络 "翻墙" 工具行为的定性分析]. 2019 3rd International Seminar on Education, Management and Social Sciences (ISEMSS 2019). Advances in Social Science, Education and Humanities Research, vol. 345 2019. 62-66.

Journal Articles

[141] AARONSON, SUSAN ARIEL: What might have been and could still be: the Trans-Pacific Partnership's potential to encourage an open internet and digital rights. *Journal of Cyber Policy*, vol. 2. no. 2. (2017) 232-254.

[142] AÇAR, KEMAL VELI: Sexual Extortion of Children in Cyberspace. *International Journal of Cyber Criminology*, vol. 10. no. 2. (2016) 110-126.

[143] AÇAR, KEMAL VELI: Webcam Child Prostitution: An Exploration of Current and Futuristic Methods of Detection. *International Journal of Cyber Criminology*, vol. 11. no. 1. (2017) 98-109.

[144] AGNEW, ROBERT: Foundation for a General Strain Theory of Crime and Delinquency. *Criminology*, vol. 30. no. 1. (1992) 47-88.

[145] AGNEW, ROBERT: Building on the Foundation of General Strain Theory: Specifying the Types of Strain Most Likely to Lead to Crime and Delinquency. *Journal of Crime and Delinquency*, vol. 38. no. 4. (2001) 319-361.

[146] AGNEW, ROBERT: Experienced, Vicarious, and Anticipated Strain: An Exploratory Study of Physical Victimization and Delinquency. *Justice Quarterly*, vol. 19. no. 4. (2002) 603-632.

[147] AGNEW, ROBERT: A General Strain Theory of Terrorism. *Theoretical Criminology*, vol. 14. no. 2. (2010) 131-153.

[148] AGNEW, ROBERT AND TIMOTHY BREZINA: Relational Problems with Peers, Gender, and Delinquency. *Youth & Society*, vol. 29. no. 1. (2007) 84-111.

[149] AJEVSKI, MARJAN: Freedom of Speech as Related to Journalists in the ECtHR, IACtHR and the Human Rights Committee – a Study of Fragmentation. *Nordic Journal of Human Rights*, vol. 32. no. 2. (2014) 118-139.

[150] AKERLOF, GEORGE A.: The Market for "Lemons": Quality Uncertainty and the Market

Mechanism. *The Quarterly Journal of Economics*, vol. 84. no. 3. (1970) 488-500.

[151] AKERS, RONALD L.: Is Differential Association/Social Learning Cultural Deviance Theory? *Criminology*, vol. 34. no. 2. (1996) 229-247.

[152] ALBONETTI, CELESTA A.: Judicial Discretion in Federal Sentencing: An Intersection of Policy priorities and Law. *Criminology & Public Policy*, vol. 10. no. 4. (2011) 1151-1155.

[153] ALÉN-SAVIKKO, ANETTE: Network neutrality in the era of 5G – a matter of faith, hope, and design? *Information & Communications Technology Law*, vol. 28. no. 2. (2019) 115-130.

[154] ALLEN, ANDREW, LEE KANNIS-DYMAND AND MARY KATSIKITIS: Problematic internet pornography use: The role of craving, desire thinking, and metacognition. *Addictive Behaviors*, vol. 70. no. (2017) 65.

[155] AL-SUWAIDI, NOURA, HAITHAM NOBANEE AND FAUZIA JABEEN: Estimating Cause of Cyber Crime: Evidence from Panel Data FGLS Estimator. *International Journal of Cyber Criminology*, vol. 12. no. 2. (2018) 392-407.

[156] AN, KE-YIN: China's Participation in the International Control of Transnational Cybercrime [跨国网络犯罪国际治理的中国参与]. *Journal of Yunnan Minzu University (Social Sciences) [云南民族大学学报(哲学社会科学版)]*, vol. 36. no. 3. (2019) 155-160.

[157] ANDERSON, GARY: The Mauerschützenprozesse and the principle of nullum crimen sine lege. *German Politics*, vol. 7. no. 2. (1998) 47-63.

[158] ANDREW, VON HIRSCH AND NILS JAREBORG: Gauging Criminal Harm: A Living-Standard Analysis. *Oxford Journal of Legal Studies*, vol. 11. no. 1. (1991) 1.

[159] BALES, WILLIAM D. AND ALEX R. PIQUERO: Racial/Ethnic Differentials in Sentencing to Incarceration. *Justice Quarterly*, vol. 29. no. 5. (2012) 742-773.

[160] BALLESTER-ARNAL, RAFAEL, JESUS CASTRO CALVO, M. DOLORES GIL-LLARIO AND BEATRIZ GIL-JULIA: Cybersex Addiction: A Study on Spanish College Students. *Journal of Sex and Marital Therapy*, vol. 43. no. 6. (2017) 567-585.

[161] BANKS, JAMES: The Heartbleed Bug: Insecurity Repackaged, rebranded and Resold. *Crime, Media, Culture*, vol. 11. no. 3. (2015) 259-279.

[162] BARGH, JOHN A. AND KATELYN Y. A. MCKENNA: The Internet and Social Life. *Annual Review of Psychology*, vol. 55. no. 1. (2004) 573-590.

[163] BAUMER, ERIC P.: Reassessing and Redirecting Research on Race and Sentencing. *Justice Quarterly*, vol. 30. no. 2. (2013) 231-261.

[164] BERGEN, EMILIA, JAN ANTFOLK, PATRICK JERN, KATARINA ALANKO AND PEKKA SANTTILA: Adults' Sexual Interest in Children and Adolescents Online: A Quasi-Experimental Study. *International Journal of Cyber Criminology*, vol. 7. no. 2. (2013) 94-111.

[165] BI, YANYING: Experimentalist approach of Chinese legislation model: From passive response to institutional design. *The Theory and Practice of Legislation*, vol. 3. no. 2. (2015) 141-167.

[166] BRADLEY-ENGEN, MINDY S., RODNEY L. ENGEN, CHRIS SHIELDS, KELLY R. DAMPHOUSSE AND BRENT L. SMITH: The Time Penalty: Examining the Relationship Between Time to Conviction and Trial vs. Plea Disparities in Sentencing. *Justice Quarterly*, vol. 29. no. 6. (2012) 829-857.

[167] BRADY, KATLYN M.: Revenge in Modern Times: The Necessity of a Federal Law Criminalizing Revenge Porn. *Hastings Women's Law Journal*, vol. 28. no. 1. (2017) 3-24.

[168] BRANTINGHAM, PAUL J. AND FREDERIC L. FAUST: A Conceptual Model of Crime Prevention. *Crime & Delinquency*, vol. 22. no. 3. (1976) 284-296.

[169] BRENNER, SUSAN W.: Nanocrime? *University of Illinois Journal of Law, Technology & Policy*, vol. 2011. no. 1. (2010) 1-74.

[170] BREWER, RUSSEL, JESSE CALE, ANDREW GOLDSMITH AND THOMAS HOLT: Young People, the Internet, and Emerging Pathways into Criminality: A Study of Australian Adolescents. *International Journal of Cyber Criminology*, vol. 12. no. 1. (2018) 115-132.

[171] BROADHURST, RODERIC: Developments in the global law enforcement of cyber‐crime. *Policing: An International Journal of Police Strategies & Management*, vol. 29. no. 3. (2006) 408-433.

[172] BURCH, TRACI: Skin Color and the Criminal Justice System: Beyond Black-White Disparities in Sentencing. *Journal of Empirical Legal Studies*, vol. 12. no. 3. (2015) 395-420.

[173] BURGESS, ROBERT L. AND RONALD L. AKERS: A Differential Association-Reinforcement Theory of Criminal Behavior. *Social Problems*, vol. 14. no. 2. (1966) 128-147.

[174] BURGESS-PROCTOR, AMANDA: Intersections of Race, Class, Gender, and Crime: Future Directions for Feminist Criminology. *Feminist Criminology*, vol. 1. no. 1. (2006) 27-47.

[175] BURMAN, MICHELE: Evidencing sexual assault: Women in the witness box. *Probation Journal*, vol. 56. no. 4. (2009) 379-398.

[176] BURRUSS, GEORGE W., ADAM M. BOSSLER AND THOMAS J. HOLT: Assessing the Mediation of a Fuller Social Learning Model on Low Self-Control's Influence on Software Piracy. *Crime & Delinquency*, vol. 59. no. 8. (2013) 1157-1184.

[177] CAI, BOHAO: Analysis of the Criminal Norm of New Internet Pornography: Based on the Live Broadcasting Obscenity Performance [新型网络色情的刑事规范分析: 以直播平台淫秽表演为切入]. *Journal of Heilongjiang Administrative Cadre Institute of Politics and Law [黑龙江省政法管理干部学院学报]*, no. 2. (2016) 24-26+30.

[178] CARAVELIS, CYNDY, TED CHIRICOS AND WILLIAM BALES: Static and Dynamic Indicators of Minority Threat in Sentencing Outcomes: A Multi-Level Analysis. *Journal of Quantitative Criminology*, vol. 27. no. 4. (2011) 405-425.

[179] CASTELLS, MANUEL: The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. *The ANNALS of the American Academy of Political and Social Science*, vol. 616. no. 1. (2008) 78-93.

[180] CHEN, XINGLIANG: From Offenses Counting to Concurrence: An Academic Advancement [从罪

数论到竞合论: 一个学术史的考察]. *Modern Law Science [现代法学]*, vol. 33. no. 3. (2011) 99-112.

[181] CHEN, YONGSHENG: The challenge and system response of cybercrime to criminal procedure [计算机网络犯罪对刑事诉讼的挑战与制度应对]. *Science of Law (Journal of Northwest University of Political Science and Law) [法律科学(西北政法大学学报)]*, vol. 32. no. 3. (2014) 140-153.

[182] CHEN, YONGSHENG: Challenges to Modern Criminal Procedure Brought by Cybercrime and Its Institutional Response [计算机网络犯罪对刑事诉讼的挑战与制度应对]. *Science of Law (Journal of Northwest University of Political Science and Law) [法律科学(西北政法大学学报)]*, vol. 32. no. 3. (2014) 140-153.

[183] CHEN, ZHENGLIANG AND RONG ZHOU: On the role and perfection of citizen network political participation in democratic political construction [论公民网络政治参与在民主政治建设中的作用及其完善]. *Academic Journal of Zhongzhou [中州学刊]*, no. 1. (2011) 17-20.

[184] CHIRCOP, LUKE: Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0. *Melbourne Journal of International Law*, vol. 20. no. 2. (2019) 349-377.

[185] CHOI, JEONG MIN, HYUN SOO NA AND JI SUK WOO: An Empirical Analysis of the Effect of the Real-Name System on Internet Bulletin Boards: How the Real-Name System and User Characteristics Influence the Use of Slanderous Comments and Swear Words. *Korean Journal of Public Administration*, vol. 48. no. 1. (2010) 71-96.

[186] CHOI, KYUNG-SHICK, SEONG-SIK LEE AND JIN REE LEE: Mobile Phone Technology and Online Sexual Harassment among Juveniles in South Korea: Effects of Self-control and Social Learning. *International Journal of Cyber Criminology*, vol. 11. no. 1. (2017) 110-127.

[187] CITRON, DANIELLE KEATS: Law's Expressive Value in Combating Cyber Gender Harassment. *Michigan Law Review*, vol. 108. no. 3. (2009) 373–415.

[188] CITRON, DANIELLE KEATS AND MARY ANNE FRANKS: Criminalizing Revenge Porn. *Wake Forest Law Review*, vol. 49. no. 2. (2014) 345-391.

[189] CLOUGH, JONATHAN: Cybercrime. *Commonwealth Law Bulletin*, vol. 37. no. 4. (2011) 671-680.

[190] CONNELL, R. W. AND JAMES W. MESSERSCHMIDT: Hegemonic Masculinity: Rethinking the Concept. *Gender & Society*, vol. 19. no. 6. (2005) 829-859.

[191] COUCH, ROBERT M.: A Suggested Legislative Approach to the Problem of Computer Crime. *Washington & Lee Law Review*, vol. 38. no. 4. (1981) 1173-1194.

[192] CRANCH, KATHRYN, CARLY M. HILINSKI-ROSICK, EMILY JOHNSON AND GABRIELA SOLANO: Revenge Pron Victimization of College Students in the United States: An Exploratory Analysis. *International Journal of Cyber Criminology*, vol. 11. no. 1. (2017) 128-142.

[193] CRANNEY, STEPHEN: Internet Pornography use and Sexual Body Image in a Dutch Sample. *International Journal of Sexual Health*, vol. 27. no. 3. (2015) 316.

[194] CRESSEY, DONALD R.: Epidemiology and Individual Conduct: A Case from Criminology. *Pacific*

Sociological Review, vol. 3. no. 2. (1960) 47-58.

[195] CRIMMINS, DANIELLE M. AND KATHRYN C. SEIGFRIED-SPELLAR: Adults who Sext: Exploring Differences in Self-Esteem, Moral Foundations, and Personality. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 169-182.

[196] CRIPPS, JENNA AND LANA STERMAC: Cyber-Sexual Violence and Negative Emotional States among Women in a Canadian University. *International Journal of Cyber Criminology*, vol. 12. no. 1. (2018) 171-186.

[197] CURRAN, JOHN F.: Internet Crime Victimization: Sentencing. *Mississippi Law Journal*, vol. 76. no. 3. (2007) 909-921.

[198] D' OVIDIO, ROB, TYSON MITMAN, IMAANI JAMILLAH EL-BURKI AND WESLEY SHUMAR: Adult-Child Sex Advocacy Websites as Social Learning Environments: A Content Analysis. *International Journal of Cyber Criminology*, vol. 3. no. 1. (2009) 421-440.

[199] DENG, HONGMEI: Current Situation, Recognition and Prevention about Network Pyramid Selling Crime in Nationality Areas [民族地区网络传销犯罪的现状、识别及预防]. *Guizhou Ethnic Studies [贵州民族研究]*, vol. 38. no. 4. (2017) 36-39.

[200] DENG, YICHENG: Can Theory of Accessorial Accomplice be Applied in Transformed Principal? [共犯正犯化背景下的从属性困境及理论应对]. *Peking University Law Journal [中外法学]*, vol. 31. no. 3. (2019) 780-796.

[201] DICKS, ANTHONY: The Chinese Legal System: Reforms In The Balance. *The China Quarterly*, vol. 119. no. (1989) 540-576.

[202] DONNELLY, ELLEN A.: The Politics of Racial Disparity Reform: Racial Inequality and Criminal Justice Policymaking in the States. *American Journal of Criminal Justice*, vol. 42. no. 1. (2017) 1-27.

[203] DRAKE, ELIZABETH K.: Benefits and Costs of "Swift, Certain, and Fair" Supervision. *Criminology & Public Policy*, vol. 17. no. 4. (2018) 865-874.

[204] DURKIN, KEITH F.: Misuse of the Internet by Pedophiles: Implications for Law Enforcement and Probation Practice. *Federal Probation*, vol. 61. no. 3. (1997) 14-18.

[205] DURKIN, KEITH F. AND CLIFTON D. BRYANT: Propagandizing Pederasty: A Thematic Analysis of the On-Line Exculpatory Accounts of Unrepentant Pedophiles. *Deviant Behavior*, vol. 20. no. 2. (1999) 103-127.

[206] EICHENSEHR, KRISTEN E.: The Cyber-Law of Nations. *Georgetown Law Journal*, vol. 103. no. 2. (2014-2015) 317-380.

[207] ENDERS, WALTER, PAUL PECORINO AND ANNE-CHARLOTTE SOUTO: Racial Disparity in U.S. Imprisonment Across States and Over Time. *Journal of Quantitative Criminology*, vol. 35. no. 2. (2019) 365-392.

[208] FANG, BINXING, PENG ZOU AND SHIBING ZHU: Research on Cyberspace Sovereignty [网络空间

主权研究]. *Chinese Journal of Engineering Science [中国工程科学]*, vol. 18. no. 6. (2016) 1-7.

[209] FEHR, CAROLINE, CHRISTINE LICALZI AND THOMAS OATES: Computer Crimes. *American Criminal Law Review*, vol. 53. no. 4 (Annual Survey of White Collar Crime). (2016) 977-1026.

[210] FEINERMAN, JAMES V.: Chinese Participation in the International Legal Order: Rogue Elephant or Team Player? *The China Quarterly*, vol. 141. (1995) 186-210.

[211] FELSON, MARCUS AND JOE L. SPAETH: Community Structure and Collaborative Consumption: "A Routine Activity Approach". *The American Behavioral Scientist*, vol. 21. no. 4. (1978) 614-624.

[212] FISCHMAN, JOSHUA B. AND MAX M. SCHANZENBACH: Racial Disparities Under the Federal Sentencing Guidelines: The Role of Judicial Discretion and Mandatory Minimums. *Journal of Empirical Legal Studies*, vol. 9. no. 4. (2012) 729-764.

[213] FLETCHER, GEORGE P.: Political theory and criminal law. *Criminal Justice Ethics*, vol. 25. no. 1. (2006) 18-38.

[214] FRANKLIN, TRAVIS W.: Sentencing Native Americans in US Federal Courts: An Examination of Disparity. *Justice Quarterly*, vol. 30. no. 2. (2013) 310-339.

[215] FRANKLIN, TRAVIS W, LAYNE DITTMANN AND TRI KEAH S HENRY: Extralegal disparity in the application of intermediate sanctions: An analysis of US district courts. *Crime & Delinquency*, vol. 63. no. 7. (2017) 839-874.

[216] FREEBORN, BETH A. AND MONICA E. HARTMANN: Judicial Discretion and Sentencing Behavior: Did the Feeney Amendment Rein in District Judges? *Journal of Empirical Legal Studies*, vol. 7. no. 2. (2010) 355-378.

[217] FREIBURGER, TINA L. AND CARLY M. HILINSKI: Probation officers' recommendations and final sentencing outcomes. *Journal of Crime and Justice*, vol. 34. no. 1. (2011) 45-61.

[218] FRISCH, WOLFGANG: From Disparity in Sentencing Towards Sentencing Equality: The German Experience. *Criminal Law Forum*, vol. 28. no. 3. (2017) 437-475.

[219] FROOMKIN, A. MICHAEL: Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases. *Journal of Law and Commerce*, vol. 15. no. 2. (1995) 395-508.

[220] FROOMKIN, A. MICHAEL: Legal Issues in Anonymity and Pseudonymity. *Information Society*, vol. 15. no. 2. (1999) 113-127.

[221] FROOMKIN, A. MICHAEL: Lessons Learned Too Well: Anonymity in a Time of Surveillance. *Arizona Law Review*, vol. 59. no. 1. (2017) 95-160.

[222] GAN, YONG: Comments on the Rules Regarding International Jurisdiction over Cyber Operations in Tallinn Manual 2.0 [《塔林手册 2.0 版》网络活动国际管辖权规则评析]. *Wuhan University International Law Review [武大国际法评论]*, vol. 3. no. 4. (2019) 117-135.

[223] GANE, NICHOLAS: The Governmentalities of Neoliberalism: Panopticism, Post-Panopticism and

beyond. *The Sociological Review*, vol. 60. no. 4. (2012) 611-634.

[224] GAO, YIFEI AND LIAN JIANG: The Development and Regulation on the Internet Real-name System. *Social Science in Guangxi*, vol. 2016. no. 2. (2016) 102-108.

[225] GEIST, MICHAEL: Cyberlaw 2.0. *Boston College Law Review*, vol. 44. no. 2. (2002) 323-358.

[226] GOLDSMITH, ANDREW AND RUSSELL BREWER: Digital drift and the criminal interaction order. *Theoretical Criminology*, vol. 19. no. 1. (2015) 112-130.

[227] GOLDSMITH, KAITLYN, CARA R. DUNKLEY, SILVAIN S. DANG AND BORIS B. GORZALKA: Pornography consumption and its association with sexual concerns and expectations among young men and women. *The Canadian Journal of Human Sexuality*, vol. 26. no. 2. (2017) 151-162.

[228] GOPAL, RAM D., G. LAWRENCE SANDERS, SUDIP BHATTACHARJEE, MANISH AGRAWAL AND SUZANNE C. WAGNER: A Behavioral Model of Digital Music Piracy. *Journal of Organizational Computing and Electronic Commerce*, vol. 14. no. 2. (2004) 89-105.

[229] GOULETTE, NATALIE, JOHN WOOLDREDGE, JAMES FRANK AND LAWRENCE TRAVIS: From Initial Appearance to Sentencing: Do Female Defendants Experience Disparate Treatment? *Journal of Criminal Justice*, vol. 43. no. 5. (2015) 406-417.

[230] GRASSIE, GILL: The Campaign Against Hate Crime Online-Can Lessons be Learned from the IP Takedown Experience to Date? *Journal of Internet Law*, vol. 21. no. 5. (2017) 3-9.

[231] GRUSEC, JOAN E.: Social Learning Theory and Developmental Psychology: The Legacies of Robert Sears and Albert Bandura. *Developmental Psychology*, vol. 28. no. 5. (1992) 776-786.

[232] GUNTER, WHITNEY D.: Internet Scallywags: A Comparative Analysis of Multiple Forms and Measurements of Digital Piracy. *Western Criminology Review*, vol. 10. no. 1. (2009) 15-28.

[233] HALL, JEROME: Nulla Poena Sine Lege. *The Yale Law Journal*, vol. 47. no. 2. (1937) 165-193.

[234] HALL, MATTHEW AND JEFF HEARN: Revenge Pornography and Manhood Acts: A Discourse Analysis of Perpetrators' Accounts. *Journal of Gender Studies*, vol. 28. no. 2. (2019) 158-170.

[235] HAMPSON, NOAH C.N.: Hacktivism: A New Breed of Protest in A Networked World. *Boston College International and Comparative Law Review*, vol. 35. no. 2. (2012) 511-542.

[236] HARMON, MARK G.: "Fixed" Sentencing: The Effect on Imprisonment Rates Over Time. *Journal of Quantitative Criminology*, vol. 29. no. 3. (2013) 369-397.

[237] HASINOFF, AMY ADELE: Sexting and Privacy Violations: A Case Study of Sympathy and Blame. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 202-217.

[238] HE, RONGGONG AND LIJIA JING: Philosophical Comments on the Excessive Use of Criminal Law for the Social Governance. *Peking University Law Journal*, vol. 3. no. 2. (2015) 401-441.

[239] HEITZEG, NANCY A.: Education or Incarceration: Zero Tolerance Policies and the School to Prison Pipeline. *Forum on Public Policy Online*, vol. 2009. no. 2. (2009) 1-21.

[240] HESTER, RHYS AND TODD K. HARTMAN: Conditional Race Disparities in Criminal Sentencing: A Test of the Liberation Hypothesis From a Non-Guidelines State. *Journal of Quantitative Criminology*, vol. 33. no. 1. (2017) 77-100.

[241] HIGGINS, GEORGE E., BRIAN D. FELL AND ABBY L. WILSON: Digital Piracy: Assessing the Contributions of an Integrated Self‐Control Theory and Social Learning Theory Using Structural Equation Modeling. *Criminal Justice Studies*, vol. 19. no. 1. (2006) 3-22.

[242] HIGGINS, GEORGE E. AND DAVID A. MAKIN: Self-Control, Deviant Peers, and Software Piracy. *Psychological Reports*, vol. 95. no. 3. (2004) 921-931.

[243] HIGGINS, GEORGE E. AND DAVID A. MAKIN: Does Social Learning Theory Condition the Effects of Low Self‐Control on College Students' Software Piracy? *Journal of Economic Crime Management*, vol. 2. no. 2. (2004) 1-22.

[244] HINDUJA, SAMEER: General Strain, Self-Control, and Music Piracy. *International Journal of Cyber Criminology*, vol. 6. no. 1. (2012) 951-967.

[245] HINDUJA, SAMEER AND JASON R. INGRAM: Social Learning Theory and Music Piracy: The Differential Role of Online and Offline Peer Influences. *Criminal Justice Studies*, vol. 22. no. 4. (2009) 405-420.

[246] HIRSCHI, TRAVIS AND MICHAEL GOTTFREDSON: Commentary: Testing the General Theory of Crime. *Journal of Research in Crime and Delinquency*, vol. 30. no. 1. (1993) 47-54.

[247] HOLLINGER, RICHARD C.: Evidence that Computer Crime Follows a Guttman-Like Progression. *Sociology and social research*, vol. 72. no. 3. (1988) 199-200.

[248] HOLLINGER, RICHARD C.: Hackers: computer heroes or electronic highwaymen? *ACM SIGCAS Computer and Society*, vol. 21. no. 1. (1991) 6–17.

[249] HOLT, TOM, JOSHUA D. FREILICH, STEVEN CHERMAK AND CLARK MCCAULEY: Political radicalization on the Internet: Extremist content, government control, and the power of victim and jihad videos. *Dynamics of Asymmetric Conflict*, vol. 8. no. 2. (2015) 107-120.

[250] HOLT, THOMAS J. AND ADAM M. BOSSLER: An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, vol. 35. no. 1. (2014) 20-40.

[251] HOLT, THOMAS J., ADAM M. BOSSLER AND DAVID C. MAY: Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice*, vol. 37. no. 3. (2012) 378-395.

[252] HOLT, THOMAS J., GEORGE W. BURRUSS AND ADAM M. BOSSLER: Social Learning and Cyber-Deviance: Examining the Importance of A Full Social Learning Model in the Virtual World. *Journal of Crime and Justice*, vol. 33. no. 2. (2010) 31-61.

[253] HONG, YU AND ERIC HARWIT: China's globalizing internet: history, power, and governance. *Chinese Journal of Communication*, vol. 13. no. 1. (2020) 1-7.

[254] HUGHES, LORINE A. AND GREGORY J. DELONE: Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both? *Social Science Computer Review*, vol. 25. no. 1. (2007) 78-98.

[255] HUREWITZ, BARRY J. AND ALLEN M. LO: Computer-Related Crimes. *American Criminal Law Review*, vol. 30. no. 3 (Annual Survey of White Collar Crime). (1993) 495-522.

[256] HURST, WILLIAM: Chinese law and governance: moving beyond responsive authoritarianism and the rule of law. *Journal of Chinese Governance*, vol. 1. no. 3. (2016) 457-469.

[257] HUSAK, DOUGLAS N. AND CRAIG A. CALLENDER: Wilful ignorance, knowledge, and the equal culpability thesis: study of the deeper significance of the principle of legality. *Wisconsin Law Review*, vol. 1994. no. 1. (1994) 29-70.

[258] IV, JOHN H. BOMAN, MARVIN D. KROHN, CHRIS L. GIBSON AND JOHN M. STOGNER: Investigating Friendship Quality: An Exploration of Self-Control and Social Control Theories' Friendship Hypotheses. *Journal of Youth and Adolescence*, vol. 41. no. 11. (2012) 1526-1540.

[259] JAISHANKA, K.: Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, vol. 1. no. 1. (2007) 1-6.

[260] JAISHANKA, K.: Sexting: A new form of Victimless Crime? *International Journal of Cyber Criminology*, vol. 3. no. 1. (2009) 21-25.

[261] JAISHANKAR, KARUPPANNAN: Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, vol. 1. no. 2. (2007) 7-9.

[262] JAISHANKAR, KARUPPANNAN: Space transition theory of cyber crimes. *Crimes of the Internet*, vol. no. (2008) 283-301.

[263] JAKOBI, ANJA P.: Non-state Actors and Global Crime Governance: Explaining the Variance of Public-private Interaction. *The British Journal of Politics and International Relations*, vol. 18. no. 1. (2016) 72-89.

[264] JIANFAN, WU: Building New China's Legal System. *Columbia Journal of Transnational Law*, vol. 22. no. 1. (1983) 1-40.

[265] JIANG, JIANGUO: Wealth Flaunt on Internet: Spiritual Poverty and Lost Values [网络炫富: 精神贫困与价值迷失]. *Modern Communication (Journal of Communication University of China) [现代传播 (中国传媒大学学报)]*, vol. 35. no. 2. (2013) 15-19.

[266] JIANZONG, YAO: The Concept of Legal Practice in the Chinese Context. *Social Sciences in China*, vol. 36. no. 3. (2015) 89-105.

[267] JIN, ZEGANG AND YA'AN WU: The Influence of online games on juvenile delinquency: an explanation based on social control theory [网络游戏对青少年犯罪的影响: 一种基于社会控制理论的解释]. *Issues on Juvenile Crimes and Delinquency [青少年犯罪问题]*, no. 5. (2012) 75-82.

[268] JINFAN, ZHANG: Ancient China's Legal Tradition and Legal Thought. *Social Sciences in China*, vol. 34. no. 2. (2013) 134-151.

[269] JING, DE JONG-CHEN: Data Sovereignty, Cybersecurity, and Challenges for Globalization. *Georgetown Journal of International Affairs*, vol. 16. no. S1. (2015) 112-122.

[270] JOHNSON, DAVID R. AND DAVID POST: Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, vol. 48. no. 5. (1995) 1367-1402.

[271] JORDAN, TIM: Language and Libertarianism: The Politics of Cyberculture and the Culture of Cyberpolitics. *The Sociological Review*, vol. 49. no. 1. (2001) 1-17.

[272] JR., RICHARD K. MOULE, DAVID C. PYROOZ AND SCOTT H. DECKER: Internet Adoption and Online Behavior among American Street Gangs: Integrating Gangs and Organizational Theory. *The British Journal of Criminology*, vol. 54. no. 6. (2014) 1186-1206.

[273] KADIR, RIZGAR MOHAMMED: The Scope and the Nature of Computer Crimes Statutes: A Critical Comparative Study. *German Law Journal*, vol. 11. no. 6. (2010) 609-632.

[274] KAMINSKI, MARGOT: Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech Articles. *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 23. no. 3. (2012) 815-896.

[275] KEITH, RONALD C.: Pitman B. Potter, China's Legal System. *Monash University Law Review*, vol. 39. no. 3. (2013) 934-940.

[276] KIM, BYUNGBAE, XIA WANG AND HYUNJUNG CHEON: Examining the Impact of Ecological Contexts on Gender Disparity in Federal Sentencing. *Justice Quarterly*, vol. 36. no. 3. (2018) 466-502.

[277] KIM, KEECHANG: Korean Internet and Real Name Verification Requirement. *Korea University Law Review*, vol. 20. no. (2016) 87-104.

[278] KOONS-WITT, BARBARA A., ERIC L. SEVIGNY, JOHN D. BURROW AND RHYS HESTER: Gender and Sentencing Outcomes in South Carolina: Examining the Interactions With Race, Age, and Offense Type. *Criminal Justice Policy Review*, vol. 25. no. 3. (2014) 299-324.

[279] KRAMER, KELSEY L. AND XIA WANG: Assessing Cumulative Disadvantage against Minority Female Defendants in State Courts. *Justice Quarterly*, vol. 36. no. 7. (2019) 1284-1313.

[280] KRASNER, STEPHEN D.: Abiding sovereignty. *International Political Science Review*, vol. 22. no. 3. (2011) 229-251.

[281] KREAGER, DEREK A.: Strangers in the Halls: Isolation and Delinquency in School Networks. *Social Forces*, vol. 83. no. 1. (2004) 351-390.

[282] KRONE, TONY: A Typology of Online Child Pornography Offending. *Trends and Issues in Crime and Criminal Justice / Australian Institute of Criminology*, vol. no. 279. (2004) 1-6.

[283] KVALEM, INGELA LUNDIN, BENTE TRÆEN AND ALEX IANTAFFI: Internet Pornography Use, Body Ideals, and Sexual Self-Esteem in Norwegian Gay and Bisexual Men. *Journal of Homosexuality*, vol. 63. no. 4. (2016) 522-540.

[284] LACOE, JOHANNA AND JILLIAN STEIN: Exploring the Policy Implications of High-Profile Police Violence. *Criminology & Public Policy*, vol. 17. no. 4. (2018) 859-863.

[285] LARSON, MATTHEW, ETHAN CANTOR, GABRIELLE CARON, ALESSANDRA LOPEZ AND DUNCAN WEALS: Computer Crimes. *American Criminal Law Review*, vol. 58. no. 3 (Annual Survey of White Collar Crime). (2021) 611-670.

[286] LARSSON, STEFAN, MÅNS SVENSSON AND MARCIN DE KAMINSKI: Online piracy, anonymity and

social change: Innovation through deviance. *Convergence*, vol. 19. no. 1. (2013) 95-114.

[287] LEE, JYH-AN AND CHING-YI LIU: Real-Name Registration Rules and the Fading Digital Anonymity in China. *Washington International Law Journal*, vol. 25. no. 1. (2016) 1-34.

[288] LEE, JIN R., THOMAS J. HOLT, GEORGE W. BURRUSS AND ADAM M. BOSSLER: Examining English and Welsh Detectives' Views of Online Crime. *International Criminal Justice Review*, (2019)

[289] LEITNER, JOHN: Identifying the Problem: Korea's Initial Experience with Mandatory Real Name Verification on Internet Portals. *Journal of Korean Law*, vol. 9. no. 1. (2009) 83-108.

[290] LESSIG, LAWRENCE: The Path of Cyberlaw Symposium: Emerging Media Technology and the First Amendment. *Yale Law Journal*, vol. 104. no. 7. (1995) 1743-1756.

[291] LI, HONG: Situational Criminology and Criminal Law Concept of Prevention [情境犯罪学与预防刑法观]. *Law Review [法学评论]*, vol. 36. no. 6. (2018) 15-28.

[292] LI, JEFFREY: Internet Control or Internet Censorship: Comparing the Control Models of China, Singapore, and the United States to Guide Taiwan's Choice. *Pittsburgh Journal of Technology Law and Policy*, vol. 14. no. 1. (2013) 1-[i].

[293] LI, LI: Nulla Poena Sine Lege in China: Rigidity or Flexibility. *Suffolk University Law Review*, vol. 43. no. 3. (2010) 655-668.

[294] LI, XIAOMING AND WENJI LI: Criminal Jurisdiction analysis of transnational cybercrime [跨国网络犯罪刑事管辖权解析]. *Journal of Soochow University (Philosophy & Social Science Edition) [苏州大学学报(哲学社会科学版)]*, vol. 39. no. 1. (2018) 89-100.

[295] LI, YONGSHENG AND WEI WU: Crime Theory of Campus Bully and its Prevention and Control Strategies: Taking China's 100 Online News in Recent Three Years as Research Samples [校园欺凌的犯罪学理论分析与防控策略: 以我国近 3 年 100 件网络新闻报道为研究样本]. *Journal of Shandong University (Philosophy and Social Sciences) [山东大学学报(哲学社会科学版)]*, no. 1. (2019) 65-74.

[296] LI, ZHONGHE: On Cyber Crimes of College Students and Its Prevention and Control Strategies [高校学生网络犯罪及其防控对策探讨]. *Science Economy Society [科学・经济・社会]*, vol. 30. no. 2. (2012) 74-78.

[297] LI, ZIYANG: The Obligation Stereotype and the Criminal Liability Determination of the Hitch Service Online Platform: Thoughts Caused by Zhengzhou Flight attendant Case and Wenzhou Preschool Teacher Case [顺风车网络平台的义务定型及刑事责任认定: 由郑州空姐案、温州幼师案引发的思考]. *Journal of Jiangxi Police Institute [江西警察学院学报]*, no. 1. (2019) 60-66.

[298] LIANG, BIN: Severe strike campaign in transitional China. *Journal of Criminal Justice*, vol. 33. no. 4. (2005) 387-399.

[299] LIANG, BIN AND HONG LU: Fighting the obscene, pornographic, and unhealthy--an analysis of the nature, extent, and regulation of China's online pornography within a global context. *Crime, Law and Social Change*, vol. 58. no. 2. (2012) 111-130.

[300] LICALZI, CHRISTINE: Computer Crime. *American Criminal Law Review*, vol. 54. no. 4. (2017) 1025-1072.

[301] LIU, JOHN ZHUANG AND XUEYAO LI: Legal Techniques for Rationalizing Biased Judicial Decisions: Evidence from Experiments with Real Judges. *Journal of Empirical Legal Studies*, vol. 16. no. 3. (2019) 630-670.

[302] LIU, SIDA: The Shape of Chinese Law. *Peking University Law Journal*, vol. 1. no. 2. (2014) 415-444.

[303] LIU, SANYANG AND CE QIN: On the Model of Cybercrime Accomplice Regulation Independent Governance [网络犯罪共犯规制独立化治理模式论]. *Chongqing Social Sciences [重庆社会科学]*, no. 7. (2019) 89-98+82.

[304] LIU, XIANQUAN: On the Theory of Quantity of Crime [罪数形态理论的正本清源]. *Chinese Journal of Law [法学研究]*, vol. 31. no. 4. (2009) 122-136.

[305] LIU, YANA AND YINGTONG GAO: An Empirical Study of Juvenile Delinquency due to Addiction to Online Games and its Coping Mechanism [青少年沉迷网络游戏及引发犯罪的实证研究与应对机制]. *Journal of Shandong University (Philosophy and Social Sciences) [山东大学学报(哲学社会科学版)]*, no. 3. (2020) 9-21.

[306] LIVINGSTONE, SONIA, KURSAT CAGILTAY AND KJARTAN OLAFSSON: EU Kids Online II Dataset: A cross-national study of children's use of the Internet and its associated opportunities and risks. *British Journal of Educational Technology*, vol. 46. no. 5. (2015) 988-992.

[307] LOVEDAY, BARRY: Still plodding along? The police response to the changing profile of crime in England and Wales. *International Journal of Police Science*, vol. 19. no. 2. (2017) 101-109.

[308] LU, HONG, BIN LIANG AND SIYU LIU: Serious Violent Offenses and Sentencing Decisions in China—Are There Any Gender Disparities? *Asian Journal of Criminology*, vol. 8. no. 3. (2013) 159-177.

[309] LU, JIANPING: Criminal Policy and Criminal Law in the Risky Society [风险社会的刑事政策与刑法]. *Legal Forum [法学论坛]*, vol. 26. no. 4. (2011) 21-25.

[310] LYNCH, MONA: Focally Concerned About Focal Concerns: A Conceptual and Methodological Critique of Sentencing Disparities Research. *Justice Quarterly*, vol. 36. no. 7. (2019) 1148-1175.

[311] LYNCH, MONA AND MARISA OMORI: Crack as Proxy: Aggressive Federal Drug Prosecutions and the Production of Black–White Racial Inequality. *Law & Society Review*, vol. 52. no. 3. (2018) 773-809.

[312] MA, EVELYN AND XIAOMENG ZHANG: Researching Chinese Law Using Legal Periodicals in

English and Chinese: A Critical Overview. *Legal Reference Services Quarterly*, vol. 34. no. 1. (2015) 1-38.

[313] MAC SÍTHIGH, DAITHÍ: The road to responsibilities: new attitudes towards Internet intermediaries. *Information & Communications Technology Law*, vol. 29. no. 1. (2020) 1-21.

[314] MACDONALD, JOHN M. AND ELLEN A. DONNELLY: Evaluating the Role of Race in Sentencing: An Entropy Weighting Analysis. *Justice Quarterly*, vol. 36. no. 4. (2017) 656-681.

[315] MAIGNAN, ISABELLE AND BRYAN A. LUKAS: The Nature and Social Uses of the Internet: A Qualitative Investigation. *The Journal of Consumer Affairs*, vol. 31. no. 2. (1997) 346-371.

[316] MAIMAITI, USMAN AND WUMAIER ABUDUMIJITI: Artificial Intelligence Algorithm Personal Information Utilization Criminal Regulations and Personal Information Security Criminal Law Protection: From New Rights to New Legal Interests [人工智能算法个人信息利用刑法规制与个人信息安全刑法保护——从新型权利转向新型法益谈起]. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition) [重庆邮电大学学报(社会科学版)]*, vol. 34. no. 1. (2022) 48-60.

[317] MAKIN, DAVID A. AND AMBER L. MORCZEK: The Dark Side of Internet Searches: A Macro Level Assessment of Rape Culture. *International Journal of Cyber Criminology*, vol. 9. no. 1. (2015) 1-23.

[318] MARCUM, CATHERINE D., GEORGE E. HIGGINS AND MELISSA L. RICKETTS: Sexting Behaviors among Adolescents in Rural North Carolina: A Theoretical Examination of Low Self-Control and Deviant Peer Association. *International Journal of Cyber Criminology*, vol. 8. no. 2. (2014) 68-78.

[319] MARCUM, CATHERINE D., GEORGE E. HIGGINS AND MELISSA L. RICKETTS: Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration *International Journal of Cyber Criminology*, vol. 8. no. 1. (2014) 47-56.

[320] MARCUM, CATHERINE D., GEORGE E. HIGGINS, MELISSA L. RICKETTS AND SCOTT E. WOLFE: Hacking in High School: Cybercrime Perpetration by Juveniles. *Deviant Behavior*, vol. 35. no. 7. (2014) 581-591.

[321] MARGANSKI, ALISON: Sexting in Poland and the United States: A Comparative Study of Personal and Social-Situational Factors. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 183-201.

[322] MARTINEZ-PRATHER, KATHY AND DONNA M. VANDIVER: Sexting among Teenagers in the United States: A Retrospective Analysis of Identifying Motivating Factors, Potential Targets, and the Role of a Capable Guardian. *International Journal of Cyber Criminology*, vol. 8. no. 1. (2014) 21-35.

[323] MAUER, MARC: Addressing the political environment shaping mass incarceration. *Criminology & Public Policy*, vol. 10. no. 3. (2011) 699-705.

[324] MCINTYRE, FRANK AND SHIMA BARADARAN: Race, Prediction, and Pretrial Detention. *Journal of Empirical Legal Studies*, vol. 10. no. 4. (2013) 741-770.

[325] MCLNTYRE-O'BRIEN, RORY: Is There Such a Thing of Cyberlaw. *Irish Student Law Review*, vol. 11. no. (2003) 118-129.

[326] MEARS, DANIEL P. AND WILLIAM D. BALES: Supermax incarceration and recidivism. *Criminology*, vol. 47. no. 4. (2009) 1131-1166.

[327] MEJIAS, ULISES A. AND NICK COULDRY: Datafication. *Internet Policy Review*, vol. 8. no. 4. (2019) 1-10.

[328] MERTON, ROBERT K.: Social Structure and Anomie. *American Sociological Review*, vol. 3. no. 5. (1938) 672-682.

[329] MI, TIENAN: The Dilemma of Accomplice Theory in Computer Network Crimes and Its Solutions [共犯理论在计算机网络犯罪中的困境及其解决方案]. *Jinan Journal (Philosophy & Social Sciences) [暨南学报(哲学社会科学版)]*, vol. 35. no. 10. (2013) 3-63+161.

[330] MOON, BYONGOOK, JOHN D. MCCLUSKEY AND CYNTHIA PEREZ MCCLUSKEY: A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice*, vol. 38. no. 4. (2010) 767-772.

[331] MORELLI, MARA, DORA BIANCHI, ROBERTO BAIOCCO, LINA PEZZUTI AND ANTONIO CHIRUMBOLO: Sexting Behaviors and Cyber Pornography Addiction Among Adolescents: The Moderating Role of Alcohol Consumption. *Sexuality Research & Social Policy*, vol. 14. no. 2. (2017) 113-121.

[332] MORRIS, ROBERT G. AND ASHLEY G. BLACKBURN: Cracking the Code: An Empirical Exploration of Social Learning Theory and Computer Crime. *Journal of Crime and Justice*, vol. 32. no. 1. (2009) 1-34.

[333] MORRIS, ROBERT G. AND GEORGE E. HIGGINS: Neutralizing Potential and Self-Reported Digital Piracy: A Multitheoretical Exploration Among College Undergraduates. *Criminal Justice Review*, vol. 34. no. 2. (2009) 173-195.

[334] MOYNIHAN, HARRIET: The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*, vol. 6. no. 3. (2021) 394-410.

[335] MUELLER, MILTON L.: Against Sovereignty in Cyberspace. *International Studies Review*, vol. 22. no. 4. (2019) 779-801.

[336] NAFTULIN, LOIS J.: The Legal Status of Women in China. *China Law Reporter*, vol. 2. no. 1. (1982) 57-60.

[337] NAGY, HABIL ZOLTÁN AND DÁVID TÓTH: Computer Related Economic Crimes in Hungary. *Journal of Eastern-European Criminal Law*, vol. 2015. no. 2. (2015) 165-174.

[338] NGO, FAWN, KARUPPANNAN JAISHANKAR AND JOSE R. AGUSTINA: Sexting: Current Research Gaps and Legislative Issues. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017)

161-168.

[339] NGO, FAWN T. AND RAYMOND PATERNOSTER: Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology*, vol. 5. no. 1. (2011) 773-793.

[340] NOBLES, MATT R., BRADFORD W. REYNS, KATHLEEN A. FOX AND BONNIE S. FISHER: Protection Against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization Among a National Sample. *Justice Quarterly*, vol. 31. no. 6. (2014) 986-1014.

[341] NOWACKI, JEFFREY S: An intersectional approach to race/ethnicity, sex, and age disparity in federal sentencing outcomes: An examination of policy across time periods. *Criminology & Criminal Justice*, vol. 17. no. 1. (2017) 97-116.

[342] O'MALLEY, TOM: Judgment and Calculation in the Selection of Sentence. *Criminal Law Forum*, vol. 28. no. 3. (2017) 361-389.

[343] O'CONNOR, KIMBERLY, MICHELLE DROUIN, NICHOLAS YERGENS AND GENNI NEWSHAM: Sexting Legislation in the United States and Abroad: A Call for Uniformity. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 218-245.

[344] OGDEN, SUZANNE: The Approach of the Chinese Communists to the Study of International Law, State Sovereignty and the International System. *The China Quarterly*, vol. 70. no. (1977) 315-337.

[345] O'NEILL, AIDAN: The EU and Fundamental Rights – Part 1. *Judicial Review*, vol. 16. no. 3. (2011) 216-247.

[346] PAINTER-DAVIS, NOAH AND JEFFERY T. ULMER: Discretion and Disparity under Sentencing Guidelines Revisited: The Interrelationship between Structured Sentencing Alternatives and Guideline Decision-making. *Journal of Research in Crime and Delinquency*, vol. no. (2019)

[347] PAN, WEIMEI AND LUCIANA DURANTI: Sitting in limbo or being the flaming Phoenix: the relevance of the archival discipline to the admissibility of digital evidence in China. *Archives and Manuscripts*, vol. 48. no. 3. (2020) 300-327.

[348] PANG, YUNXIA AND LI SUN: On Criminal Regulations on Online Obscene Live Streaming [论网络色情直播的刑法规制]. *Journal of Changchun Normal University [长春师范大学学报]*, vol. 37. no. 7. (2018) 40-43.

[349] PARK, K. S.: Mandatory Identity Verification in the Internet: Did Google Do the Right Thing. *Korea University Law Review*, vol. 5. (2009) 203-224.

[350] PASSAS, NIKOS: Anomie and Corporate Deviance. *Contemporary Crises*, vol. 14. no. 2. (1990) 157-178.

[351] PASSAS, NIKOS: Global Anomie, Dysnomie, and Economic Crime: Hidden Consequences of Neoliberalism and Globalization in Russia and Around the World. *Social Justice*, vol. 27. no. 2. (2000) 16-44.

[352] PATTERSON, EVELYN J.: Hidden Disparities: Decomposing Inequalities in Time Served in

California, 1985–2009. *Law & Society Review*, vol. 49. no. 2. (2015) 467-498.

[353] PEI, WEI: The Connection of the Electronic Forensics Rules before and after Criminal Recording: From the Perspective of Procedural Nature of Electronic Evidence [刑事立案前后电子取证规则衔接问题研究: 以电子数据证据过程性为视角]. *Contemporary Law Review [当代法学]*, vol. 33. no. 2. (2019) 114-126.

[354] PILS, EVA: Resisting Dignity Takings in China. *Law & Social Inquiry*, vol. 41. no. 4. (2016) 888-916.

[355] PINA-SÁNCHEZ, J. AND R. LINACRE: Enhancing Consistency in Sentencing: Exploring the Effects of Guidelines in England and Wales. *Journal of Quantitative Criminology*, vol. 30. no. 4. (2014) 731-748.

[356] POOLE, JAY AND RYAN MILLIGAN: Nettersexuality: The Impact of Internet Pornography on Gay Male Sexual Expression and Identity. *Sexuality & Culture*, vol. 22. no. 4. (2018) 1189-1204.

[357] POTTER, PITMAN B.: The Chinese Legal System: Continuing Commitment to the Primacy of State Power. *The China Quarterly*, vol. 159. (1999) 673-683.

[358] PRATT, TRAVIS C. AND FRANCIS T. CULLEN: The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis. *Criminology*, vol. 38. no. 3. (2000) 931-964.

[359] PRATT, TRAVIS C., FRANCIS T. CULLEN, CHRISTINE S. SELLERS, L. THOMAS WINFREE, TAMARA D. MADENSEN, LEAH E. DAIGLE, NOELLE E. FEARN AND JACINTA M. GAU: The Empirical Status of Social Learning Theory: A Meta‐Analysis. *Justice Quarterly*, vol. 27. no. 6. (2010) 765-802.

[360] QIU, LING: Analysis on Crime of Refusing to Perform the Obligation of Information Network Security Management [拒不履行信息网络安全管理义务罪探析]. *Law Science Magazine [法学杂志]*, vol. 41. no. 4. (2020) 64-71.

[361] QUINN, JAMES F. AND CRAIG J. FORSYTH: Red Light Districts on Blue Screens: A Typology for Understanding the Evolution of Deviant Communities on the Internet. *Deviant Behavior*, vol. 34. no. 7. (2013) 579-585.

[362] RAITIO, JUHA: Legal Certainty, Non-Retroactivity and Periods of Limitation in EU Law. *Legisprudence*, vol. 2. no. 1. (2008) 1-23.

[363] RANDOLPH, JUSTUS: A Guide to Writing the Dissertation Literature Review. *Practical Assessment, Research, and Evaluation*, vol. 14. no. 13. (2009) 1-14.

[364] RICHARDS, TARA N., M. DWAYNE SMITH, WESLEY G. JENNINGS, BETH BJERREGAARD AND SONDRA J. FOGEL: An Examination of Defendant Sex Disparity in Capital Sentencing: A Propensity Score Matching Approach. *American Journal of Criminal Justice*, vol. 39. no. 4. (2014) 681-697.

[365] ROBERTS, JOSHUA W. AND SCOTT A. HUNT: Social Control in a Sexually Deviant Cybercommunity: A Cappers' Code of Conduct. *Deviant Behavior*, vol. 33. no. 10. (2012) 757-773.

[366] RODRIGUEZ, LAURIE J. AND DAVID E. BARLOW: Structural contradictions and the United States Sentencing Commission. *Crime, Law and Social Change*, vol. 32. no. 2. (1999) 169-202.

[367] ROSÉN, FREDERIK: Towards a Theory of Institutionalized Judicial Exceptionalism. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, vol. 6. no. 2. (2005) 147-163.

[368] ROWBOTTOM, JACOB: The transformation of obscenity law. *Information & Communications Technology Law*, vol. 27. no. 1. (2018) 4-29.

[369] RUGE, GERD: An Interview with Chinese Legal Officials. *The China Quarterly*, vol. 61. (1975) 118-126.

[370] SADOWSKI, JATHAN: When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, vol. 6. no. 1. (2019) 1-12.

[371] SÁNCHEZ, VIRGINIA, NOELIA MUÑOZ-FERNÁNDEZ AND ESTHER VEGA-GEA: Peer sexual cybervictimization in adolescents: Development and validation of a scale. *International Journal of Clinical and Health Psychology*, vol. 17. no. 2. (2017) 171-179.

[372] SANCHEZ-OSTIZ, PABLO: Towards a Re-Principled Criminal Law. *Transnational Legal Theory*, vol. 5. no. 4. (2014) 511-540.

[373] SAVIRIMUTHU, JOSEPH: Rethinking Cyberlaw: A New Vision for Internet Law Book Review. *SCRIPTed: Journal of Law, Technology and Society*, vol. 13. no. 3. (2016) 393-397.

[374] SCHINASI, JOHN: Practicing Privacy Online: Examining Data Protection Regulations through Google's Global Expansion Note. *Columbia Journal of Transnational Law*, vol. 52. no. 2. (2013) 569-616.

[375] SCHMITT, MICHAEL N. AND LIIS VIHUL: Sovereignty in cyberspace: Lex lata vel non? *AJIL Unbound*, vol. 111. (2017) 213-218.

[376] SCHMITT, MICHAEL N. AND LIIS VIHUL: Respect for Sovereignty in Cyberspace. *Texas Law Review*, vol. 95. no. 7. (2017) 1639-1670.

[377] SCHMITZ, SANDRA: Facebook's Real Name Policy: Bye-Bye, Max Mustermann? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC)*, vol. 4. no. 3. (2013) 190-204.

[378] SCULLEN, CAMERON RYAN: Cyberspace: The 21st Century Battlefield. *University of Miami National Security and Armed Conflict Law Review*, vol. 6. no. (2016) 233-264.

[379] SEIGFRIED-SPELLAR, KATHRYN: Individual Differences of Internet Child Pornography Users: Peculiar Findings in a Community-Based Study. *International Journal of Cyber Criminology*, vol. 7. no. 2. (2013) 141-154.

[380] SELA-SHAYOVITZ, REVITAL: Gangs and the Web: Gang Members' Online Behavior. *Journal of Contemporary Criminal Justice*, vol. 28. no. 4. (2012) 389-405.

[381] SHAN, DAN AND LAI WANG: The application of big data in the investigation of online illegal fund-raising cases [大数据在网络非法集资案件侦查中的应用]. *Journal of People's Public*

Security University of China (Social Sciences Edition) [中国人民公安大学学报(社会科学版)], vol. 33. no. 4. (2017) 84-91.

[382] SHEN, YI: Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, vol. 1. no. 1. (2016) 81-93.

[383] SIMON, GLENN E.: Cyberporn and censorship: Constitutional barriers to preventing access to Internet pornography by minors. *Journal of Criminal Law & Criminology*, vol. 88. no. 3. (1998) 1015-1048.

[384] SIRIANNI, JOSEPH M. AND ARUN VISHWANATH: Problematic Online Pornography Use: A Media Attendance Perspective. *The Journal of Sex Research*, vol. 53. no. 1. (2016) 21.

[385] SKINNER, WILLIAM F. AND ANNE M. FREAM: A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, vol. 34. no. 4. (1997) 495-518.

[386] SOLOVE, DANIEL J.: Digital Dossiers and the Dissipation of Fourth Amendment Privacy. *Southern California Law Review*, vol. 75. no. 5. (2002) 1083-1168.

[387] SOMMER, JOSEPH H.: Against Cyberlaw. *Berkeley Technology Law Journal*, vol. 15. no. 3. (2000) 1145-1232.

[388] SONG, DAWEI: The Criminal Governance of 'QR Code' Crime [二维码犯罪的刑事治理]. *Journal of Heilongjiang Administrative Cadre College of Politics and Law [黑龙江省政法管理干部学院学报]*, no. 5. (2017) 32-35.

[389] SONG, DAWEI: What is Cybercrime? A criminology Perspective. *Public Goods and Governance*, vol. 3. no. 2. (2018) 10-15.

[390] SONG, DAWEI: Sentencing Disparity in China: A descriptive Research on Auxiliary Cybercrime Stipulated by Amendment IX of criminal law. *Iustum Aequum Salutare*, vol. XVII. no. 2. (2021) 209-239.

[391] SPIGELMAN, JAMES J.: The Principle of Legality and the Clear Statement Principle. *Australian Law Journal*, vol. 79. (2005) 769.

[392] SPOHN, CASSIA: Evolution of Sentencing Research. *Criminology & Public Policy*, vol. 14. no. 2. (2015) 225-232.

[393] SPOHN, CASSIA C., BYUNGBAE KIM, STEVEN BELENKO AND PAULINE K. BRENNAN: The Direct and Indirect Effects of Offender Drug Use on Federal Sentencing Outcomes. *Journal of Quantitative Criminology*, vol. 30. no. 3. (2014) 549-576.

[394] STANLEY, NICKY, CHRISTINE BARTER, MARSHA WOOD, NADIA AGHTAIE, CATH LARKINS, ALBA LANAU AND CAROLINA ÖVERLIEN: Pornography, Sexual Coercion and Abuse and Sexting in Young People's Intimate Relationships: A European Study. *Journal of Interpersonal Violence*, vol. 33. no. 19. (2018) 2919-2944.

[395] STARR, TEGAN S. AND TIFFANY LAVIS: Perceptions of Revenge Pornography and Victim Blame.

International Journal of Cyber Criminology, vol. 12. no. 2. (2018) 427-438.

[396] STEFFENSMEIER, DARRELL, NOAH PAINTER-DAVIS AND JEFFERY ULMER: Intersectionality of Race, Ethnicity, Gender, and Age on Criminal Punishment. *Sociological Perspectives*, vol. 60. no. 4. (2017) 810-833.

[397] STEINBERG, STACEY: Changing faces: Morphed child pornography images and the first amendment. *Emory Law Journal*, vol. 68. no. 5. (2019) 909-938.

[398] STEINMETZ, KEVIN F. AND KENNETH D. TUNNELL: Under the Pixelated Jolly Roger: A Study of On-Line Pirates. *Deviant Behavior*, vol. 34. no. 1. (2013) 53-67.

[399] STRATE, LANCE: The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, vol. 63. no. 3. (1999) 382-412.

[400] SUN, DAOCUI: Coordinated development between criminal governance and Network Register System [网络实名制与刑事治理的协同化思考]. *Journal of Nanjing University of Post and Telecommunication (Volume of Social Science) [南京邮电大学学报(社会科学版)]*, vol. 18. no. 3. (2013) 16-24.

[401] SUN, WEI AND QICHAO ZHU: A Primary Study on ASEAN Cyber Security Cooperation [东盟网络安全合作现状与展望]. *Southeast Asian Studies [东南亚研究]*, no. 1. (2016) 56-64.

[402] SUN, YUNLIANG: Dogmatics Introspection on the Principal Offenderization of Helping Behavior [帮助行为正犯化的教义学反思]. *Journal of Comparative Law [比较法研究]*, vol. no. 6. (2018) 120-133.

[403] SUTHERLAND, EDWIN H.: Is "White Collar Crime" Crime? *American Sociological Review*, vol. 10. no. 2. (1945) 132-139.

[404] SWEENY, JOANNE AND JOHN SLACK: Sexting as 'Sexual Behavior' Under Rape Shield Laws. *International Journal of Cyber Criminology*, vol. 11. no. 2. (2017) 246-260.

[405] SYKES, GRESHAM M. AND DAVID MATZA: Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, vol. 22. no. 6. (1957) 664-670.

[406] TABER, JOHN K.: On Computer Crime (Senate Bill S. 240). *Computer/Law Journal*, vol. 1. no. (1978-1979) 517-544.

[407] TAY, ALICE ERH-SOON: Law in Communist China - Part 1. *Sydney Law Review*, vol. 6. no. 2. (1968) 153-172.

[408] TAYLOR, PAUL A.: From hackers to hacktivists: speed bumps on the global superhighway? *New Media & Society*, vol. 7. no. 5. (2005) 625-646.

[409] THORNTON, PATRICIA M.: Of Constitutions, Campaigns and Commissions: A Century of Democratic Centralism under the CCP. *The China Quarterly*, vol. 248. no. S1. (2021) 52-72.

[410] TIAN, SHENGBIN: On the Jurisdiction System of Internet Criminal Cases [互联网刑事案件管辖制度研究]. *Tribune of Political Science and Law [政法论坛]*, vol. 39. no. 3. (2021) 36-48.

[411] TILLYER, ROB, RICHARD D. HARTLEY AND JEFFREY T. WARD: Differential Treatment of Female

Defendants: Does Criminal History Moderate the Effect of Gender on Sentence Length in Federal Narcotics Cases? *Criminal Justice and Behavior*, vol. 42. no. 7. (2015) 703-721.

[412] TONG, YUNFENG: Research on the Regulation Limit of Cyber Crawler Behavior in Big Data Age [大数据时代网络爬虫行为刑法规制限度研究]. *Journal of Dalian University of Technology (Social Science) [大连理工大学学报(社会科学版)]*, vol. 43. no. 2. (2022) 88-97.

[413] TUTTLE, JAMES C.: Developments in China's Legal System: Introduction and Delegation Overview. *China Law Reporter*, vol. 2. no. 1. (1982) 36-56.

[414] ULMER, JEFFERY T: Recent developments and new directions in sentencing research. *Justice Quarterly*, vol. 29. no. 1. (2012) 1-40.

[415] ULMER, JEFFERY T: Criminal courts as inhabited institutions: Making sense of difference and similarity in sentencing. *Crime and Justice*, vol. 48. no. 1. (2019) 483-522.

[416] VAN DER SLOOT, BART: How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one. *Information & Communications Technology Law*, vol. 24. no. 1. (2015) 74-103.

[417] WALDRON, JEREMY: Legislation and the Rule of Law. *Legisprudence*, vol. 1. no. 1. (2007) 91-123.

[418] WALL, DAVID S.: Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime. *International Review of Law, Computers & Technology*, vol. 22. no. 1-2. (2008) 45-63.

[419] WANG, GONGZHENG: Criminal Regulation of Erotic Behavior on Live Online Platform [网络直播平台色情行为的刑法规制]. *Journal of Nanjing University of Aeronautics and Astronautics (Social Sciences) [南京航空航天大学学报(社会科学版)]*, vol. 20. no. 1. (2018) 52-57.

[420] WANG, HUIBO: Social learning theory of our country from the perspective of white-collar crime analysis [社会学习理论视角的我国白领犯罪解析]. *Henan Social Science [河南社会科学]*, vol. 20. no. 8. (2012) 52-55.

[421] WANG, JIANBO: An Empirical Research on Regional Disparity of Bribery Crime Sentencing in China [我国受贿罪量刑地区差异问题实证研究]. *China Legal Science [中国法学]*, vol. no. 4. (2016) 245-265.

[422] WANG, LIN: Shaping from Dogmatics for Criminal Liability Mode for Participative Conduct of Cybercrime [网络犯罪参与行为刑事责任模式的教义学塑造: 共犯归责模式的回归]. *Political Science and Law [政治与法律]*, no. 9. (2016) 30-42.

[423] WANG, LIMEI: The Construction of Summary Procedure of Judicial Assistance of Cross Border Electronic Evidence [论跨境电子证据司法协助简易程序的构建]. *Law Science Magazine [法学杂志]*, vol. 41. no. 3. (2020) 82-92.

[424] WANG, SUZHI: On the Principal Quality of Cybercrime Participation: Rethinking Based on the

Offence of Assisting Cybercrime [论网络犯罪参与行为的正犯性: 基于帮助信息网络犯罪活动罪的反思]. *Journal of Comparative Law [比较法研究]*, no. 1. (2020) 170-184.

[425] WANG, SUZHI: The Model Controversy of International Legislation on Cybercrime and China's Plan [网络犯罪国际立法的模式之争与中国方案]. *Nanjing University Law Journal [南大法学]*, no. 5. (2021) 107-124.

[426] WANG, WEI: Singapore's Cyberspace Governance and Its Enlightenment to China [论新加坡网络空间治理及对中国的启示]. *Pacific Journal [太平洋学报]*, vol. 26. no. 2. (2018) 35-45.

[427] WANG, XIA AND DANIEL P. MEARS: Sentencing and State-Level Racial and Ethnic Contexts. *Law & Society Review*, vol. 49. no. 4. (2015) 883-915.

[428] WANG, XIA, DANIEL P. MEARS, CASSIA SPOHN AND LISA DARIO: Assessing the Differential Effects of Race and Ethnicity on Sentence Outcomes Under Different Sentencing Systems. *Crime*, vol. 59. no. 1. (2013) 87-114.

[429] WANG, YING: On discussion of the social effects caused by wealth flaunt advertising [试论炫富广告引发的社会效应]. *Lanzhou Academic Journal [兰州学刊]*, no. S1. (2008) 153-154.

[430] WANG, ZHENHUI: The Crime of Minor's Social Networking: Risk Type and Prevention Measures [未成年人网络社交中的犯罪被害: 风险类型与防范之策]. *Journal of Chinese Youth Social Science [中国青年社会科学]*, vol. 39. no. 6. (2020) 120-127.

[431] WARD, GEOFF, AMY FARRELL AND DANIELLE ROUSSEAU: Does Racial Balance in Workforce Representation Yield Equal Justice? Race Relations of Sentencing in Federal Court Organizations*. *Law & Society Review*, vol. 43. no. 4. (2009) 757-806.

[432] WEI, YUEJIANG: How Countries Around The World Implement Internet Real-Name System. *Shanghai Informatization*, vol. 2013. no. 3. (2013) 82-86.

[433] WEN, FENGMING AND XUEFANG XIE: The operation logic and ethical concerns of the short video recommendation algorithm: Based on the Actor Network Theory [短视频推荐算法的运行逻辑与伦理隐忧: 基于行动者网络理论视角]. *Journal of Southwest Minzu University (Humanities and Social Science) [西南民族大学学报 (人文社会科学版)]*, vol. 43. no. 2. (2022) 160-169.

[434] WEST, CANDACE AND DON H. ZIMMERMAN: Doing Gender. *Gender & Society*, vol. 1. no. 2. (1987) 125-151.

[435] XIA, YU AND GUOQIANG LIU: The Criminal Regulations of the Internet Pornography Live Broadcast [论网络色情直播行为的刑法规制]. *Journal of Hubei Engineering University [湖北工程学院学报]*, vol. 42. no. 1. (2022) 95-101.

[436] XIAO, YINGYING AND ZHENGQING YUAN: A Primary Exploration on Cyber Security Governance in Africa [非洲网络安全治理初探]. *West Asia and Africa [西亚非洲]*, no. 3. (2016) 121-137.

[437] XIE, DENGKE: Rethink and Reconstruction of the Online Extraction Rules of Electronic Evidence [电子数据网络在线提取规则反思与重构]. *Oriental Law [东方法学]*, no. 3. (2020) 89-100.

[438] XIE, HONGREN: Restore the Truth: Traditional Chinese Law and Its Distortion by the Western Knowledge System. *International Critical Thought*, vol. 5. no. 3. (2015) 296-312.

[439] XIE, WANGYUAN: On the Crime of Refusing to Fulfill the Obligation of Information Network Security Administration [论拒不执行信息网络安全管理义务罪]. *China Legal Science [中国法学]*, no. 2. (2017) 238-255.

[440] XIN, YANYU AND TIANJI CAI: Paying money for freedom: Effects of monetary compensation on sentencing for criminal traffic offenses in China. *Journal of Quantitative Criminology*, (2019)

[441] XINXIANG, ZHANG: A Study on the Non-Statutory Factors in Death Penalty Trials in China. *Peking University Law Journal*, vol. 2. no. 2. (2014) 317-353.

[442] XU, LINGBO: The System Position and Principle of Criminal Concurrence: The German Concurrence Theory as a Reference [犯罪竞合的体系位置与原则: 以德国竞合理论为参照]. *Journal of Comparative Law [比较法研究]*, no. 6. (2017) 86-97.

[443] XU, SHANPIN AND SHUCHENG WANG: Australia's Cyber Security Strategy in the Digital Age: New Connotation and New Trend [澳大利亚网络安全战略的新内涵与新动向]. *Journal of International Security Studies [国际安全研究]*, vol. 37. no. 6. (2019) 104-128+155-166.

[444] YAMAGUCHI, ITSUKO: Cyberlaw. *Theory, Culture & Society*, vol. 23. no. 2-3. (2006) 529-531.

[445] YANG, ZHIPING: An Analysis of Adolescent Cyber Pornography Consciousness [青少年网络色情犯罪意识生成分析]. *Youth Exploration [青年探索]*, no. 4. (2014) 84-88.

[446] YAR, MAJID: Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal of Criminal Justice*, vol. 44. no. 4. (2005) 387-399.

[447] YAU, HON-MIN: Fragmenting Cyberspace and Constructing Cyber Norms: China's Efforts to Reshape Global Cyber Governance. *Contemporary Chinese Political Economy and Strategic Relations*, vol. 7. no. 2. (2021) 691-715, XII.

[448] YOU, WEI AND XIMEI XIE: The Principle of Trust and its Application in the Negligent Crimes [信赖原则及其在过失犯罪中的运用]. *Science of Law (Journal of Northwest University of Political Science and Law) [法律科学(西北政法大学学报)]*, no. 5. (2001) 56-65.

[449] YOUNG, KIMBERLY: Understanding Sexually Deviant Online Behavior from an Addiction Perspective. *International Journal of Cyber Criminology*, vol. 2. no. 1. (2008) 298-307.

[450] YU, HAISONG: The Recent Development of the Criminal Procedure Rules of Cybercrime: Based on the "Interpretation of the New Criminal Procedure Law" [网络犯罪刑事程序规则的新近发展: 基于《新刑事诉讼法解释》的解读]. *China Journal of Applied Jurisprudence [中国应用法学]*, no. 5. (2021) 51-61.

[451] YU, XINGZHONG: Legal Pragmatism in the People's Republic of China. *Journal of Chinese Law*, vol. 3. no. 1. (1989) 29-52.

[452] YU, ZHIGANG: The Standpoint of China in Concluding and Participating in the International

Convention on Cyberspace [缔结和参加网络犯罪国际公约的中国立场]. *Tribune of Political Science and Law [政法论坛]*, vol. 33. no. 5. (2015) 91-108.

[453] YUAN, SHUGUANG: Sociological analysis of crime of Internet pornography, gambling and drugs [网络黄赌毒犯罪的社会学分析]. *Dongyue Tribune [东岳论丛]*, vol. 33. no. 7. (2012) 179-181.

[454] ZENG, YONG, XIAOJIANG LI AND WENQI ZHAO: Detection Model of Concealed Conspiracy in Enterprise Based on Social Network Analysis and Fuzzy Comprehensive Evaluation Method [基于社会网络分析的企业隐藏犯罪探测的模糊评价模型]. *Journal of Modern Information [现代情报]*, vol. 32. no. 7. (2012) 103-106.

[455] ZHANG, MINGKAI: Distinctions Between the Overlap of Articles of Law and the Imaginative Joiner of Offenses [法条竞合与想象竞合的区分]. *Chinese Journal of Law [法学研究]*, vol. 38. no. 1. (2016) 127-147.

[456] ZHANG, WENWEI: Information Security Cooperation under Shanghai Cooperation Organization: Necessity, Current Situation, and Prospect [上海合作组织信息安全合作: 必要性、现状及前景]. *Russian, East European & Central Asian Studies [俄罗斯东欧中亚研究]*, vol. 3. no. 5. (2016) 94-106.

[457] ZHANG, XU AND XIAOYAN ZHU: Crime Governance in Weak Smart Society: Situation, Dilemma, and Settlement Paths [弱智慧社会语境下的犯罪治理: 情势、困境与出路]. *Jilin University Journal Social Sciences Edition [吉林大学社会科学学报]*, vol. 59. no. 1. (2019) 19-29+219.

[458] ZHAO, BINGZHI AND QIWEI ZHAN: Formation of Crime regarding Nonfulfillment of Secure and Manage Obligation on Information System and Network [论拒不执行信息网络安全管理义务罪的罪过形式]. *Guizhou Social Sciences [贵州社会科学]*, vol. 360. no. 12. (2019) 61-67.

[459] ZHAO, JIAXIANG: Comprehensively Understanding of the Relationship between Theory and Practice [全面理解理论和实践的关系]. *Journal of China Executive Leadership Academy Yan'an [中国延安干部学院学报]*, no. 2. (2017) 27-35.

[460] ZHAO, XINGHONG: The Application of Probation in China: An Empirical Study using Chinese Judicial Documents [缓刑适用的中国图景: 基于裁判文书大数据的实证研究]. *Contemporary Law Review [当代法学]*, vol. 31. no. 2. (2017) 46-61.

[461] ZHENG, CHUNRONG AND XIAOSHAN NI: EU Cybersecurity Strategy and China-EU Cooperation [欧盟网络安全战略及中欧合作]. *Journal of Tongji University (Social Science Section) [同济大学学报(社会科学版)]*, vol. 31. no. 4. (2020) 42-56.

[462] ZHENG, ZESHAN: Cybercrime and the Principle of the Validity in terms of Space in Criminal Law [网络犯罪与刑法的空间效力原则]. *Chinese Journal of Law [法学研究]*, no. 5. (2006) 71-81.

[463] ZHOU, YANYAN, BRYANT PAUL, VINCENT MALIC AND JINGYUAN YU: Sexual behavior patterns in online sexually explicit materials: a network analysis. *Quality & Quantity*, vol. 53. no. 4. (2019)

2253-2271.

[464] ZHU, JINGWEN: The Socialist Legal System with Chinese Characteristics: Its Structure, Features and Trends. *Social Sciences in China*, vol. 32. no. 3. (2011) 87-103.

[465] ZHU, SHIBING, XUEBO ZHANG, YU WANG AND YUNJIE LIU: A Review of Major Viewpoints on Cyber Sovereignty around the World [世界范围内网络主权的主要观点综述]. *Chinese Journal of Engineering Science [中国工程科学]*, vol. 18. no. 6. (2016) 89-93.

[466] ZHU, WEI: Research on the Progress of Internet Broadcast Technology [互联网直播技术研究]. *Modern Information Technology [现代信息科技]*, vol. 2. no. 10. (2018) 104-106.

Web pages and Online Materials

[467] Picture Reading | About "Building a Community of Shared Future in Cyberspace Together" President Xi Jinping said at the World Internet [读图 | 关于"共同构建网络空间命运共同体"习近平主席在世界互联网大会上这样说], World Internet Conference, 2021. 4 November, https://2020.wicwuzhen.cn/web20/wlqg/

[468] President Xi Jinping's views on the Internet, World Internet Conference, 2021. 4 November, http://www.wuzhenwic.org/2015-12/11/c_548266.htm

[469] People born after 1990 are the main victims of telecom and Internet fraud ["90 后""00 后"成电信网络诈骗主要受害群体], 2021. 4 November, http://digital.china.com.cn/2021-08/30/content_41658840.htm

[470] Popular information, NobelPrize.org., 2022. 13 March, https://www.nobelprize.org/prizes/economic-sciences/2001/popular-information/

[471] Morphology, Merriam-Webster, 2022. 14 March, https://www.merriam-webster.com/dictionary/morphology#note-1

[472] What is Morphology? All About Linguistics, 2022. 14 March, https://all-about-linguistics.group.shef.ac.uk/branches-of-linguistics/morphology/what-is-morphology/

[473] Cybercrime: Global Programme on Cybercrime, United Nations Office on Drugs and Crime, 2022. 15 March, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

[474] Wu Bangguo's speech at the Fourth Session of the Eleventh National People's Congress [吴邦国在第十一届全国人民代表大会第四次会议上的讲话], The National People's Congress of The People's Republic of China, 2022. 20 March, http://www.npc.gov.cn/zgrdw/npc/dbdhhy/11_4/2011-07/06/content_1871271.htm

[475] Jiang Zemin's report at the 15th National Congress of the Communist Party of China [江泽民在中国共产党第十五次全国代表大会上的报告], 12371.cn, 2022. 20 March, https://fuwu.12371.cn/2012/09/27/ARTI1348726215537612_all.shtml

[476] An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?

CCDCOE: The NATO Cooperative Cyber Defence Centre of Excellence, 2022. 24 March, https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/

[477] Ministry of Industry and Information Technology: Internet companies are not allowed to automatically or forcefully download APPs without user consent [工信部：互联网企业未经用户同意不得自动或强制下载 APP], stdaily.com, 2022. 3 March, http://www.stdaily.com/index/kejixinwen/202203/23f191e515894989875494886f4a9883.shtml

[478] First Maneuver of Cyber Anti-terrorism in Shanghai Cooperation Organization [上合组织首次演练网络反恐], Xinhua News Agency, 2019. 2 May, http://www.xinhuanet.com//politics/2015-10/15/c_128318903.htm

[479] CYBERSPACE ADMINISTRATION OF CHINA (CAC): Cyberspace Administration of China releases Digital China Development Report 2020 [国家互联网信息办公室发布《数字中国发展报告（2020 年）》], 2021. 3 July, http://www.gov.cn/xinwen/2021-07/03/content_5622668.htm

[480] CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION (CIGI): Global Commission on Internet Governance (2014–2016): About the GCIG, CIGI, 2022. 25 March, https://www.cigionline.org/activities/global-commission-internet-governance-2014-2016/

[481] INTERNET CRIME COMPLAINT CENTER (IC3): 2020 Internet Crime Report, Federal Bureau of Investigation, 2021. 11 November, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[482] BANDURA, ALERT: Social Learning Theory, General Learning Process, 2021. 23 October, https://web.archive.org/web/20131024214846/http://www.jku.at/org/content/e54521/e54528/e54529/e178059/Bandura_SocialLearningTheory_ger.pdf

[483] BBC NEWS: Didi Chuxing suspends carpool service after woman killed, BBC, 2019. 1 April, https://www.bbc.com/news/world-asia-china-45313074

[484] BBC NEWS: China car app Didi updates safety measures after murder, BBC, 2019. 1 April, https://www.bbc.com/news/technology-44143297

[485] BOTSMAN, RACHEL: The case for collaborative consumption, TED, 2019. 1 April, https://www.ted.com/talks/rachel_botsman_the_case_for_collaborative_consumption

[486] CCTV NEWS: China is “one of the most secure countries in the world” The national public security index in 2020 is 98.4% [中国是“世界上最有安全感的国家之一”2020 年全国群众安全感指数 98.4%], CCTV. COM, 2021. 12 November, https://news.cctv.com/2021/04/15/ARTIAuqN0sAjdiQh6rGWd15y210415.shtml

[487] CENTRAL COMMITTEE OF THE COMMUNIST PARTY OF CHINA: Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Upholding and Improving the Socialist System with Chinese Characteristics and Promoting the Modernization of the National Governance System and Governance Ability [中共中央关于坚持和完善中国特色社会

主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定], Xinhua News Agency, 2019. 31 October, http://www.xinhuanet.com/2019-11/05/c_1125195786.htm

[488] CHAI, WESLEY: What is a hacker? TechTarget, 2021. 28 October, https://www.techtarget.com/searchsecurity/definition/hacker

[489] CHINA DAILY: Thousands busted in identity theft cases, China Daily, 2018. 25 December, http://www.chinadaily.com.cn/china/2013-05/30/content_16547114.htm

[490] CHINA INTERNET NETWORK INFORMATION CENTER(CNNIC): The 42nd Statistical Report on Internet Development in China, China Internet Network Information Center(CNNIC), 2018. 1 October, http://www.cnnic.com.cn/IDR/ReportDownloads/201911/P020191112538212107066.pdf

[491] CHINA JUSTICE BIG DATA ACADEMY: Features and Trends of Cybercrime (2016.1-2018.12), China Justice Big Data Service Platform, 2019. 19 November, https://pdfs.semanticscholar.org/ee29/6776064640534a9041f5856051b15fd6ef76.pdf

[492] CHRIS DEZIEL: The Effects of a Small Sample Size Limitation, 2018. 13 March, https://sciencing.com/effects-small-sample-size-limitation-8545371.html

[493] CYBERSECURITY VENTURES: The 2019 Official Annual Cybercrime Report, Herjavec Group, 2019. 19 March, https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

[494] DAIGLE, LESLIE: On the Nature of the Internet, Centre for International Governance Innovation and Chatham House, 2022. 13 March, https://www.cigionline.org/static/documents/gcig_paper_no7.pdf

[495] DIDI: About us, DiDi. Inc, 2019. 1 April, https://www.didiglobal.com/about-didi/about-us

[496] DINGTALK: Which Companies Are Using Ding Talk? [哪些企业在用钉钉?], Ding Talk, 2022. 17 March, https://www.dingtalk.com/qidian/help-detail-20288922.html

[497] DU, XIAO AND ZIXUAN FU: Legal Rules And Technical Rules Need To Blend With Each Other [法律规则与技术规则需彼此交融], Legal Daily, 2018. 11 December, http://legal.people.com.cn/n1/2018/0921/c42510-30306323.html

[498] EUROPOL: Internet organised crime threat assessment (IOCTA) 2019, 2019. 9 October, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

[499] FINDLAW'S TEAM OF LEGAL WRITERS AND EDITORS: Reverse Discrimination, FindLaw, 2021. 28 October, https://www.findlaw.com/employment/employment-discrimination/reverse-discrimination.html

[500] FRENCH, SALLY: China has 9 of the world's 20 biggest tech companies, Market Watch, 2018. 13 December, https://www.marketwatch.com/story/china-has-9-of-the-worlds-20-biggest-tech-companies-2018-05-31

[501] GU, YONGZHONG: The meaning of "trial-centered" as it should be [“以审判为中心”的应然

涵 义], Procuratorial Daily, 2019. 11 December, http://newspaper.jcrb.com/2019/20191211/20191211_003/20191211_003_3.htm

[502] GUANGMING NET: Tmall Double 11 calendar year turnover summary, Sohu News, 2021. 9 November, https://www.sohu.com/na/431088718_162758

[503] IIMEDIA RESEARCH CENTER: 2019 H1 China Online Living Streaming Market Research Report, iiMedia Research Inc, 2019. https://report.iimedia.cn/report.jsp?reportId=38871

[504] KELLAND, MARK: Social Learning Theory and Personality Development, openstax CNX: Personality Theory in a Cultural Context, 2021. 23 October, https://cnx.org/contents/lISyy6OT@1.1:oiev6HcT@1/Social-Learning-Theory-and-Personality-Development

[505] LEINER, BARRY M., VINTON G. CERF, DAVID D. CLARK, ROBERT E. KAHN, LEONARD KLEINROCK, DANIEL C. LYNCH, JON POSTEL, LARRY G. ROBERTS AND STEPHEN WOLFF: Brief History of the Internet, Internet Society, 2021. 11 November, https://www.internetsociety.org/internet/history-internet/brief-history-internet/

[506] LI, KEQIANG: Government Work Report of 2015, The State Council of People's Republic of China, 2021. 11 November, http://www.gov.cn/guowuyuan/2015-03/16/content_2835101.htm

[507] LI, KEQIANG: Government Work Report of 2020, The State Council of People's Republic of China, 2021. 11 November, http://www.gov.cn/guowuyuan/2020zfgzbg.htm

[508] LILLEMOSE, JACOB AND MATHIAS KRYGER: The (Re)invention of Cyberspace, Kunstkritikk, 2018. 5 November, https://kunstkritikk.com/the-reinvention-of-cyberspace/

[509] LUO, HUANHUAN: 50 Sexual Invasion Sample Cases and “DIDI Rectification” [50个性侵犯样本与“滴滴整改”], infzm.com, 2019. 1 April, http://www.infzm.com/contents/136003

[510] MERRIAM-WEBSTER DICTIONARY: Definition of Cyber, Merriam-Webster Dictionary, 2021. 15 November, https://www.merriam-webster.com/dictionary/cyber

[511] MILMO, DAN: Enter the metaverse: the digital future Mark Zuckerberg is steering us toward, The Guardian, 2021. 11 November, https://www.theguardian.com/technology/2021/oct/28/facebook-mark-zuckerberg-meta-metaverse

[512] MINISTRY OF FOREIGN AFFAIRS OF THE PEOPLE’S REPUBLIC OF CHINA: China and Russia sign an international information security cooperation agreement, Ministry of Foreign Affairs of the People’s Republic of China, 2019. 2 May, https://www.fmprc.gov.cn/web/wjbz_673089/xghd_673097/t1263088.shtml

[513] MINISTRY OF JUSTICE OF THE PEOPLE’S REPUBLIC OF CHINA: About us: What We Do, Ministry of Justice of the People’s Republic of China, 2021. 17 November, http://en.moj.gov.cn/2019-06/20/c_383604.htm

[514] MOFFITT, KIMBERLY AND JEFFREY PERRY: Social Conflict Theory in Sociology: Definition & Contributors, Study.com, 2021. 26 October, https://study.com/academy/lesson/social-conflict-

theory-in-sociology-definition-lesson-quiz.html

[515] NATIONAL INSTITUTE OF JUSTICE OF U.S. DEPARTMENT OF JUSTICE: Computer Crime: Criminal Justice Resource Manual (Second Edition), 1989. August, https://files.eric.ed.gov/fulltext/ED332671.pdf

[516] OFFICE OF LEGAL EDUCATION: Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, 2021. 16 November, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

[517] QUEST MOBILE: Quest Mobile China Mobile Internet 2020 Annual Report (Part 2): Mobile Internet Industry Inventory [Quest Mobile 中国移动互联网 2020 年度大报告 (下篇): 移动互联网行业盘点], Quest Mobile, 2021. 2 February, https://www.questmobile.com.cn/research/report-new/143

[518] RAUHALA, EMILY: Uber loses bid for China business, plans to merge with main rival, The Washington Post, 2019. 1 April, https://www.ndtv.com/world-news/uber-loses-bid-for-china-business-plans-to-merge-with-main-rival-1438797

[519] RAY, JULIE: Most of the World Remains Confident in Police, Feels Safe, Gallup, 2021. 12 November, https://news.gallup.com/poll/322565/world-remains-confident-police.aspx

[520] ROSS, SEAN: Theory of Asymmetric Information, Investopedia, 2022. 13 March, https://www.investopedia.com/ask/answers/042415/what-theory-asymmetric-information-economics.asp

[521] SCO RATS: About SCO RATS: History, Regional Anti-terrorist Structure of Shanghai Cooperation Organisation, 2022. 24 March, https://ecrats.org/en/history/

[522] SHANGHAI COOPERATION ORGANIZATION: About SCO, SCO Secretariat, 2019. 19 March, http://eng.sectsco.org/about_sco/

[523] SHDF NATIONAL OFFICE: SHDF National Office deployed the "CleanNet 2019", "NursingSeedling 2019" and "AutumnWind 2019" Special Action [全国"扫黄打非"办公室部署开展"净网 2019""护苗 2019""秋风 2019"专项行动], 2019. 4 March, http://www.shdf.gov.cn/shdf/contents/767/394202.html

[524] SHDF NATIONAL OFFICE: About us, 2019. 20 October, http://www.shdf.gov.cn/shdf/contents/749/236131.html

[525] SHDF NATIONAL OFFICE: Guang Xi Province: The city of Nan Ning rendered a judgment about online obscene live streaming [广西：南宁市宣判一起网络直播淫秽表演案], 2019. 19 June, http://www.shdf.gov.cn/shdf/contents/11420/401368.html

[526] SHDF NATIONAL OFFICE: Si Chuan: The city of Le Shan investigated a case of utilizing phone software to broadcast online pornographic live shows [四川：乐山市查办一起利用手机直播软件进行网上传播淫秽色情案件], 2019. 31 May, http://www.shdf.gov.cn/shdf/contents/11419/401357.html

[527] SHDF NATIONAL OFFICE: Zhe Jiang: The court in the city of Ja Xing adjudicated a case of making criminal profits by disseminating online pornography through the Nebula Platform [浙江：嘉兴市“星云直播”平台传播淫秽物品牟利案宣判], 2019. 17 June, http://www.shdf.gov.cn/shdf/contents/11420/399777.html

[528] SHDF NATIONAL OFFICE: Jiang Xi: The court in the city of Jiu Jiang sentenced the ‘6.05’ case of gaining criminal profits by disseminating online pornography through an online live streaming platform [江西：九江市判结“6·05”网络直播平台传播淫秽物品牟利案], 2019. 19 September, http://www.shdf.gov.cn/shdf/contents/11419/405296.html

[529] SHDF NATIONAL OFFICE: Hu Bei: The police knocked out the transnational criminal gang of online obscene live streaming. The illegal gains were 16 million, and 20 people were arrested [湖北：警方打掉跨国网络色情直播团伙 牟利 1600 万 20 人落网], 2019. 30 May, http://www.shdf.gov.cn/shdf/contents/11419/400064.html

[530] SHIH, GERRY: China taxi apps Didi Dache and Kuaidi Dache announce $6 billion tie-up, Reuters, 2019. 1 April, https://www.reuters.com/article/us-china-taxi-merger-idUSKBN0LI04420150214

[531] SOHU FINANCE: Shocked!!! The SCO has become the most populous and largest regional cooperative organization in the world [震惊!!! 上合组织成为世界上人口最多、面积最大的地区合作组织了], Sohu News, 2019. 20 March, https://www.sohu.com/a/149073133_169746

[532] SOHU NEWS: Juveniles watch pornography on the website. Upload “inventory” to become an administrator [少年为在网站多看黄片 上传“库存”争当管理员] Parents report and expose porn sites to the police [家长报警曝光黄色网站], 2019. 26 October, http://news.sohu.com/20140630/n401556398.shtml

[533] SONG, YU: [World Vision] The Rise and Fall of South Korean Network Real-Name System [天下远见：韩国网络实名制兴废记], infzm.com, 2018. 24 December, http://www.infzm.com/contents/67455

[534] SUPREME PEOPLE’S COURT: Sentencing Guideline for Common Crimes [最高人民法院关于常见犯罪的量刑指导意见], Supreme People’s Court, 2014. 31 July, http://www.court.gov.cn/shenpan-xiangqing-6622.html

[535] SUPREME PEOPLE’S COURT: Provisions on People’s Courts Publishing Judgment Documents on the Internet [关于人民法院在互联网公布裁判文书的规定], 2016. 31 August, http://www.court.gov.cn/zixun-xiangqing-25321.html

[536] SUPREME PEOPLE’S COURT: Press conference on the ‘Interpretations of the supreme people's court and supreme people's procuratorate on the application of laws in handling criminal cases of illegal utilizing information network technology and assisting cyber-criminal activities’ [《最高人民法院、最高人民检察院关于办理非法利用信息网络帮助信息网络、犯罪活动等刑事案

件适用法律若干问题的解释》新闻发布会], 2019. 25 October, http://www.court.gov.cn/zixun-xiangqing-193671.html

[537] TENCENT: Tiktok Has 400 Million Daily Active Users, Wechat Has 1 Billion, and You May Not Think of Alipay's Number [抖音日活 4 亿，微信 10 亿，支付宝日活可能你想不到], Tencent, 2020. 13 January, https://xw.qq.com/amphtml/20200113A0S6V300

[538] THE WORLD BANK: GDP Ranking: Gross Domestic Product Ranking Table, The World Bank, 2021. 12 November, https://datacatalog.worldbank.org/search/dataset/0038130/GDP-ranking

[539] WANG, PAN, SISI XIAO AND YING ZHOU: A verdict was pronounced in the "Gene Edited Baby" case. He Jiankui and other three defendants were held criminally responsible [“基因编辑婴儿”案一审宣判 贺建奎等三被告人被追究刑事责任], Xinhua News Agency, 2019. 30 December, http://www.xinhuanet.com/2019-12/30/c_1125403802.htm

[540] XINHUA NEWS: China's "sharing economy" up 103 pct in 2016: report, Xinhua News Agency, 2019. 1 April, http://www.xinhuanet.com//english/2017-03/05/c_136104460.htm

[541] XINHUA NEWS: Xinhua News criticizes the phenomenon of short video platform showing off wealth: this extravagant trend should be taken care of! [新华社批短视频平台炫富现象: 这股奢靡之风该管管了], Xinhua News Agency, 2021. 21 October, https://finance.sina.com.cn/china/2021-04-15/doc-ikmxzfmk7034255.shtml

[542] XINHUA NEWS: Xi Jinping delivered a congratulatory speech to the first World Internet Conference [习近平向首届世界互联网大会致贺词], World Internet Conference, 2021. 4 November, https://2019.wicwuzhen.cn/web19/wlqg/zwln/201908/t20190822_10862142.shtml

[543] XINING POLICE (XINING MUNICIPAL BUREAU OF PUBLIC SECURITY OF QINGHAI PROVINCE OF CHINA): Common telecom fraud routines are all in these 10 pictures! [常见的电信诈骗套路，全在这 10 张图里!], thepaper.cn, 2022. 12 March, https://m.thepaper.cn/newsDetail_forward_2840882

[544] XUEERSHIXI: Xi Jinping: The Internet is not a place outside the law, QSTHEORY. cn, 2021. 4 November, http://www.qstheory.cn/zhuanqu/2021-10/13/c_1127952040.htm?ivk_sa=1023197a

[545] YE, QIAN: Telecom fraud "scenario" has been renovated so quickly, users become "stunned birds" [电信诈骗“剧本”翻新神速 用户成“惊弓之鸟”], Xinhua News Agency, 2021. 21 October, http://www.cac.gov.cn/2016-01/02/c_1117649793.htm

[546] ZHANG, JUN: Work Report of the Supreme People's Procuratorate of 2021, The Supreme People's Procuratorate of The People's Republic of China, 2021. 21 November, https://www.spp.gov.cn/spp/gzbg/202103/t20210315_512731.shtml

[547] ZHANG, YI AND XIN QI: Didi suspends 'hitch' service after driver allegedly kills passenger, China Daily, 2019. 1 April, http://www.chinadaily.com.cn/a/201805/12/WS5af62b55a3103f6866ee7ec5.html

[548] ZHOU, QIANG: Work Report of the Supreme People's Court of 2021, The Supreme People's Court of The People's Republic of China, 2021. 21 November, http://www.court.gov.cn/zixun-xiangqing-290831.html

LIST OF PUBLICATIONS OF THE PH.D. CANDIDATE

UNIVERSITY of DEBRECEN

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

Registry number: DEENK/182/2022.PL
Subject: PhD Publication List

Candidate: Dawei Song
Doctoral School: Géza Marton Doctoral School of Legal Studies
MTMT ID: 10067720

List of publications related to the dissertation

Articles, studies (6)

1. **Song, D.**: Rethinking the Evolution of Terminologies of Defining Cybercrime Outside China.
   Kexue yu jishu = Journal of Science and Technology. "Accepted by Publisher" (-), 1-4, 2022. ISSN: 1003-9716.

2. **Song, D.**: Sentencing Disparity in China: A Descriptive Research on Auxiliary Cybercrime Stipulated by Amendment IX of Criminal Law.
   Iustum aequum salutare. 17 (2), 209-239, 2021. ISSN: 1787-3223.

   Level of HAS Committee on Legal and Political Sciences: A

3. **Song, D.**: Criminal Risk for Online-Platform of Sharing Economy: From the DiDi Hitch Service Case Study in China.
   Public Goods and Governance. 4 (1), 16-22, 2019. EISSN: 2498-6453.

   Level of HAS Committee on Legal and Political Sciences: D

4. **Song, D.**: Internet Real-name System and Cybercrime Prevention in China: a Critical Perspective.
   Jura. 25 (2), 470-481, 2019. ISSN: 1218-0793.

   Level of HAS Committee on Legal and Political Sciences: A

5. **Song, D.**: New legislation or new interpretation on cybercrime: on the analysis of online obscene live streaming in China.
   Jog, állam, politika. 11 (4), 55-75, 2019. ISSN: 2060-4580.

   Level of HAS Committee on Legal and Political Sciences: A

6. **Song, D.**: What is Cybercrime?: A Criminology Perspective.
   Public Goods and Governance. 3 (2), 11-15, 2018. EISSN: 2498-6453.

   Level of HAS Committee on Legal and Political Sciences: D

DEBRECENI EGYETEM Egyetemi és Nemzeti Könyvtár

UNIVERSITY AND NATIONAL LIBRARY
UNIVERSITY OF DEBRECEN
H-4002 Egyetem tér 1, Debrecen
Phone: +3652/410-443, email: publikaciok@lib.unideb.hu

Conference presentations (3)

7. **Song, D.**: Regional International Organization on Cooperation of Combating Cybercrime: Shanghai Cooperation Organization and China.
   In: Tavaszi Szél = Spring Wind 2019. Szerk.: Bihari Erika, Molnár Dániel, Szikszai-Németh Ketrin, Doktoranduszok Országos Szövetsége, Budapest, 358-363, 2020. ISBN: 9786155586606
8. **Song, D.**: A Brief Introduction: China's Legal Systems on Cyberspace Governance.
   In: Doktoranduszok fóruma : Állam- és Jogtudományi Kar szekciókiadványa. Szerk.: Szabó Miklós, Miskolci Egyetem Állam- és Jogtudományi Kar, Miskolc, 17-24, 2019. ISBN: 9789633581919
9. **Song, D.**: Internet Real-name System in China: Policy, Doctrine, and Principle.
   In: XIV. Jogász Doktoranduszok Országos Szakmai Találkozója 2018. Szerk.: Miskolczi Bodnár Péter, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest, 375-382, 2019. ISBN: 9786155961021

By the directives of HAS Committee on Legal and Political Sciences:

Publications in periodicals level „A": 3, related to the dissertation: 3.

Publications in periodicals level „D": 2, related to the dissertation: 2.

The Candidate's publication data submitted to the iDEa Tudóstér have been validated by DEENK on the basis of the Journal Citation Report (Impact Factor) database.

12 April, 2022

DEBRECENI EGYETEM Egyetemi és Nemzeti Könyvtár